SRIDA IT PROFESSIONAL REFERENCE PUBLICATION · FREE EDITION

CIS Controls v8.1

CIS Critical Security Controls · with an India lens · Free Edition

Implementation Guidance & Assessment Testing Procedures

DOCUMENT ID	VERSION	STATUS
SRIDA-CIS-RTP-001	1.0	Final — Approved for Publication

Rajendra Bodda
Chief Information Security Officer (CISO)
Srida IT · 2026

Independent professional guidance.
Not a CIS publication.



CIS Critical Security Controls v8.1 — with an India Lens

Implementation Guidance & Assessment Testing Procedures

Prepared by

Rajendra Bodda

Chief Information Security Officer (CISO)

Published by Srida IT

SRIDA-CIS-RTP-001 · Version 1.0 · November 2026

This publication is an independently developed professional guidance document prepared by Srida IT and distributed free of charge. It is not a publication of the Center for Internet Security, Inc. (CIS), is not affiliated with or endorsed by CIS or any Indian regulator, is not legal advice and does not confer any certification. The CIS Controls are © Center for Internet Security and licensed under CC BY-NC-ND 4.0; only the Controls as published by CIS at https://www.cisecurity.org/controls/ are authoritative.

Document Information and Control

Field	Value
Document title	CIS Critical Security Controls v8.1 — with an India Lens
Subtitle	Implementation Guidance & Assessment Testing Procedures
Document identifier	SRIDA-CIS-RTP-001
Version	1.0
Status	Final — Approved for Publication
Classification	Srida IT Professional Reference Publication · Free Edition
Author	Rajendra Bodda, Chief Information Security Officer (CISO)
Publisher	Srida IT
Publication year	2026
Issue date	November 2026
Reference document	Center for Internet Security, CIS Critical Security Controls Version 8.1, June 2024, https://www.cisecurity.org/controls/ (licensed CC BY-NC-ND 4.0)
Related documents	ISO/IEC 27001:2022; NIST CSF 2.0 (CSWP 29); NIST SP 800-53 Rev. 5; CERT-In Directions of 28 April 2022; SEBI CSCRF (2024); RBI IT governance directions; DPDP Act 2023 and DPDP Rules 2025
Companion publications	SRIDA-NIST-CSF-RTP-001; SRIDA-ISMS-27001-RTP-001; SRIDA-ATTR-27028-RTP-001; SRIDA-DPDP-RTP-001
Next review	On a new CIS Controls version, and at least annually

Version history

Version	Date	Author	Description of change
1.0	November 2026	Rajendra Bodda	First published edition, approved for publication.

Approval

Role	Name	Date
Approved for publication	Rajendra Bodda, Chief Information Security Officer (CISO)	29 November 2026

Distribution

Released for publication by Srida IT. Distribution and use are subject to the permitted-use terms in the Copyright, Legal and Usage Notices.

Copyright, Legal and Usage Notices

DISCLAIMER

This publication is an independently developed professional guidance document prepared by Srida IT and distributed free of charge. It is not a publication of the Center for Internet Security, Inc. (CIS), is not affiliated with or endorsed by CIS or any Indian regulator, is not legal advice and does not confer any certification. The CIS Controls are © Center for Internet Security and licensed under CC BY-NC-ND 4.0; only the Controls as published by CIS at https://www.cisecurity.org/controls/ are authoritative.

COPYRIGHT AND LICENCE

© 2026 Srida IT. The original content of this publication (its structure, interpretations, implementation guidance, testing procedures, templates, examples and tables) is the work of Rajendra Bodda for Srida IT. It is made available free of charge under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International licence (CC BY-NC-ND 4.0, https://creativecommons.org/licenses/by-nc-nd/4.0/): you may copy and share it unmodified, for non-commercial purposes, with credit to Srida IT.

CIS CONTROLS ATTRIBUTION

The CIS Critical Security Controls® are © Center for Internet Security, Inc. (CIS®) and licensed under CC BY-NC-ND 4.0 (https://creativecommons.org/licenses/by-nc-nd/4.0/). This publication quotes only the Control and Safeguard titles, asset types, security functions and Implementation Group assignments of CIS Controls v8.1, unmodified, for identification; all explanation is in Srida IT's own words and is not a modified version of the Controls. For the authoritative and most up-to-date Controls, refer to https://www.cisecurity.org/controls/. Commercial use of the CIS Controls is subject to the prior approval of CIS.

NO AFFILIATION, ENDORSEMENT OR CERTIFICATION

Srida IT is not affiliated with, endorsed by or a partner of CIS, and is not affiliated with any Indian regulator. There is no CIS Controls certification for organisations, and use of this publication does not result in, guarantee or imply compliance with any law or regulation, or certification against any standard.

SAFEGUARDS VERSUS GUIDANCE VERSUS RECOMMENDATIONS

This publication distinguishes the CIS Safeguards (identified by their CIS titles), related practice from other frameworks, and Srida IT recommended practice. Testing procedures, sample sizes, evaluation indicators, maturity indicators, crosswalks, regulatory touchpoints, templates and examples are Srida IT's recommended practice.

EXAMPLES

All organisations, systems, people, findings and figures in examples are fictional.

PERMITTED USE

This free edition may be downloaded, used within any organisation for reference, implementation, assessment and training, and shared unmodified for non-commercial purposes. The templates in Part V may be completed and adapted for your own internal use. Selling this publication, or using it in paid training or consulting products, is not permitted.

PROFESSIONAL ADVICE

This publication provides general professional guidance. It is not legal, regulatory or audit-opinion advice and does not create a client, consulting or advisory relationship. Organisations should apply professional judgement in tailoring any guidance to their mission, risk appetite, sector and regulatory obligations.

LIMITATION OF LIABILITY

This publication is provided "as is" without warranties of any kind, express or implied, including accuracy, completeness, currency or fitness for a particular purpose. To the fullest extent permitted by applicable law, Srida IT and the author shall not be liable for any direct, indirect, incidental, special or consequential loss or damage, including any adverse assessment or regulatory outcome, arising from the use of, or reliance on, this publication.

CONFIDENTIALITY OF COMPLETED MATERIAL

Completed Profiles, Tier worksheets, gap analyses, workpapers and assessment reports prepared using this publication will contain sensitive security information and must be protected under the organisation's classification scheme.

TRADEMARKS

CIS®, CIS Controls® and CIS Critical Security Controls® are registered trademarks of the Center for Internet Security, Inc. NIST, ISO, IEC and other names mentioned are trademarks or registered marks of their respective owners and are used only for identification, without implying affiliation or endorsement.

ACCURACY AND CURRENCY

Information is believed accurate as of November 2026 and reflects CIS Controls v8.1 (June 2024). The Controls, CIS's online resources and Indian regulatory instruments continue to evolve; verify against current official sources.

About the Author and Publisher

Rajendra Bodda

Chief Information Security Officer (CISO), Srida IT

Rajendra Bodda leads information security, governance, risk and compliance at Srida IT. This manual draws on practical experience of implementing and assessing cybersecurity programmes for organisations serving Indian and international clients.

About Srida IT

Srida IT is an information security and GRC consulting organisation focused on building digital trust through practical governance, risk and compliance programmes. Contact: sridait.com · info@sridait.com

Feedback

Corrections and suggestions for future editions are welcome at info@sridait.com, quoting the document identifier SRIDA-CIS-RTP-001 and the section reference.

Table of Contents

Part I Foundations 14

Chapter 1 Introduction to the CIS Controls v8.1 15
Chapter 2 Structure: Controls, Safeguards, Asset Classes, Security Functions 19
Chapter 3 Implementation Groups in Depth: Choosing Your IG 24
Chapter 4 The CIS Controls and Related Frameworks 30
Chapter 5 Terminology and Abbreviations 35
Chapter 6 How to Use This Manual and the Assessment Method 41

Part II The 18 CIS Controls 47

Chapter 7 Control 1: Inventory and Control of Enterprise Assets 48
Control 1 Inventory and Control of Enterprise Assets 48
Chapter 8 Control 2: Inventory and Control of Software Assets 56
Control 2 Inventory and Control of Software Assets 56
Chapter 9 Control 3: Data Protection 64
Control 3 Data Protection 64
Chapter 10 Control 4: Secure Configuration of Enterprise Assets and Software 77
Control 4 Secure Configuration of Enterprise Assets and Software 77
Chapter 11 Control 5: Account Management 89
Control 5 Account Management 89
Chapter 12 Control 6: Access Control Management 98
Control 6 Access Control Management 98
Chapter 13 Control 7: Continuous Vulnerability Management 108
Control 7 Continuous Vulnerability Management 108
Chapter 14 Control 8: Audit Log Management 117
Control 8 Audit Log Management 117
Chapter 15 Control 9: Email and Web Browser Protections 129
Control 9 Email and Web Browser Protections 129
Chapter 16 Control 10: Malware Defenses 138
Control 10 Malware Defenses 138
Chapter 17 Control 11: Data Recovery 148
Control 11 Data Recovery 148
Chapter 18 Control 12: Network Infrastructure Management 157
Control 12 Network Infrastructure Management 157
Chapter 19 Control 13: Network Monitoring and Defense 168
Control 13 Network Monitoring and Defense 168
Chapter 20 Control 14: Security Awareness and Skills Training 180
Control 14 Security Awareness and Skills Training 180
Chapter 21 Control 15: Service Provider Management 190
Control 15 Service Provider Management 190
Chapter 22 Control 16: Application Software Security 200
Control 16 Application Software Security 200
Chapter 23 Control 17: Incident Response Management 213

Control 17 Incident Response Management 213

Chapter 24 Control 18: Penetration Testing 224

Control 18 Penetration Testing 224

Part III Implementation 233

Chapter 25 IG1 Essential Cyber Hygiene: a 90-Day Roadmap 234

Chapter 26 Growing into IG2 and IG3 239

Chapter 27 Tooling, Automation and Secure Configuration Baselines 243

Chapter 28 One Control Set: CIS with ISO/IEC 27001, NIST CSF 2.0 and Indian Regulation 248

Chapter 29 The CIS Controls for SMEs, Start-ups and Managed Service Providers 253

Part IV Assessment 257

Chapter 30 Running a CIS Controls Assessment 258

Chapter 31 Assessment Techniques and Evidence 263

Chapter 32 Findings, Reporting and Improvement 268

Part V Appendices and Templates 272

Appendix A Safeguard Matrix 273

Appendix B Control Summary 278

Appendix C IG1 Self-Assessment Checklist 279

Appendix D Implementation Status Worksheet 283

Appendix E Gap Analysis and 12-Month Action Plan 290

Appendix F CIS Controls v8.1 to ISO/IEC 27001:2022 Crosswalk 293

Appendix G India Regulatory Touchpoints Matrix 297

Appendix H Completed Assessment Workpaper (Control 5) 300

Appendix I Board Reporting Template 306

Appendix J References 309

List of Tables

Table 1-1	Main versions of the CIS Controls	15
Table 1-2	The 18 CIS Controls v8.1 and their Safeguard counts	17
Table 2-1	The six v8.1 asset classes	19
Table 2-2	Safeguards per Control by asset class (v8.1)	20
Table 2-3	The six security functions and their Safeguard counts (v8.1)	21
Table 2-4	Safeguards per Control by security function (v8.1)	22
Table 2-5	Asset class by security function (v8.1)	22
Table 3-1	Safeguards in each Implementation Group (v8.1)	24
Table 3-2	Safeguards per Control applicable at each IG (cumulative, v8.1)	25
Table 3-3	New Safeguards at each IG by security function (v8.1)	26
Table 3-4	New Safeguards at each IG by asset class (v8.1)	26
Table 3-5	Factors for choosing a target Implementation Group (Srida IT guidance)	27
Table 3-6	Illustrative IG choices for fictional Indian enterprises	27
Table 4-1	How the CIS Controls differ from related frameworks	30
Table 4-2	CIS Controls v8.1 to ISO/IEC 27001:2022 Annex A (Srida IT Control-level mapping)	31
Table 4-3	CIS Controls v8.1 to NIST CSF 2.0 Categories (Srida IT orientation)	32
Table 4-4	Principal Indian instruments and the CIS Controls they draw on most	32
Table 4-5	One activity, many frameworks: an example for Safeguard 11.4	34
Table 5-1	Terms used in this manual	35
Table 5-2	Abbreviations used in this manual	38
Table 6-1	Parts of this manual and who they serve	41
Table 6-2	Sections of each Control chapter	41
Table 6-3	Testing methods used in this manual	43
Table 6-4	Safeguard evaluation scale	43
Table 6-5	Default minimum sample sizes (Srida IT guidance)	44
Table 7-1	Safeguards of CIS Control 1, Inventory and Control of Enterprise Assets	48
Table 7-2	Assessment testing procedures, Control 1	52
Table 8-1	Safeguards of CIS Control 2, Inventory and Control of Software Assets	56
Table 8-2	Assessment testing procedures, Control 2	60
Table 9-1	Safeguards of CIS Control 3, Data Protection	64
Table 9-2	Assessment testing procedures, Control 3	72
Table 10-1	Safeguards of CIS Control 4, Secure Configuration of Enterprise Assets and Software	77
Table 10-2	Assessment testing procedures, Control 4	84
Table 11-1	Safeguards of CIS Control 5, Account Management	89
Table 11-2	Assessment testing procedures, Control 5	93
Table 12-1	Safeguards of CIS Control 6, Access Control Management	98
Table 12-2	Assessment testing procedures, Control 6	103
Table 13-1	Safeguards of CIS Control 7, Continuous Vulnerability Management	108
Table 13-2	Assessment testing procedures, Control 7	113
Table 14-1	Safeguards of CIS Control 8, Audit Log Management	117
Table 14-2	Assessment testing procedures, Control 8	124
Table 15-1	Safeguards of CIS Control 9, Email and Web Browser Protections	129
Table 15-2	Assessment testing procedures, Control 9	134
Table 16-1	Safeguards of CIS Control 10, Malware Defenses	138
Table 16-2	Assessment testing procedures, Control 10	144
Table 17-1	Safeguards of CIS Control 11, Data Recovery	148
Table 17-2	Assessment testing procedures, Control 11	153
Table 18-1	Safeguards of CIS Control 12, Network Infrastructure Management	157

Table 18-2	Assessment testing procedures, Control 12	163
Table 19-1	Safeguards of CIS Control 13, Network Monitoring and Defense	168
Table 19-2	Assessment testing procedures, Control 13	175
Table 20-1	Safeguards of CIS Control 14, Security Awareness and Skills Training	180
Table 20-2	Assessment testing procedures, Control 14	186
Table 21-1	Safeguards of CIS Control 15, Service Provider Management	190
Table 21-2	Assessment testing procedures, Control 15	196
Table 22-1	Safeguards of CIS Control 16, Application Software Security	200
Table 22-2	Assessment testing procedures, Control 16	208
Table 23-1	Safeguards of CIS Control 17, Incident Response Management	213
Table 23-2	Assessment testing procedures, Control 17	219
Table 24-1	Safeguards of CIS Control 18, Penetration Testing	224
Table 24-2	Assessment testing procedures, Control 18	229
Table 25-1	1 — The 56 IG1 Safeguards arranged into a 90-day plan (Srida IT sequencing)	236
Table 25-2	2 — Week-by-week IG1 schedule for a firm with part-time IT support	237
Table 26-1	1 — Signals that an enterprise should target IG2 or IG3 (Srida IT guidance)	239
Table 26-2	2 — New Safeguards added at IG2 and IG3, by Control (from canon)	239
Table 26-3	3 — Two dimensions of progress that must be reported separately	242
Table 27-1	1 — Vendor-neutral tool categories and the Controls they support	243
Table 27-2	2 — Automating recurring Safeguard activities	245
Table 27-3	3 — Example IG1 baseline outline for company laptops	246
Table 28-1	1 — CIS Controls v8.1 to ISO/IEC 27001:2022 Annex A, summary crosswalk (Srida IT mapping)	248
Table 28-2	2 — Selected CIS Safeguards and related NIST CSF 2.0 Subcategories (Srida IT mapping)	249
Table 28-3	3 — Indian obligations and the CIS Controls that support them (Srida IT mapping; mapping is not compliance)	250
Table 29-1	1 — Low-cost IG2 Safeguards worth considering early in a small firm (Srida IT guidance)	253
Table 29-2	2 — Example responsibility split for IG1 Safeguards between an SME customer and its MSP	255
Table 30-1	1 — Typical target choices for fictional India-angle enterprises (Srida IT guidance)	259
Table 30-2	2 — The evaluation scale applied to each Safeguard	259
Table 30-3	3 — Example score calculation for an IG1 self-assessment	260
Table 31-1	1 — Testing methods used in this manual	263
Table 31-2	2 — Guideline sample sizes for CIS Controls testing (Srida IT guidance)	264
Table 31-3	3 — Evidence types and their relative reliability	265
Table 31-4	4 — Example tests for Indian regulatory parameters linked to the Safeguards	266
Table 32-1	1 — Structure of a finding	268
Table 32-2	2 — Finding risk ratings (Srida IT scale)	268
Table 32-3	3 — Example board dashboard summary	270
Table 32-4	4 — Misleading and accurate wording	270
Table A-1	Safeguard matrix	273
Table B-1	Control summary	278
Table C-1	IG1 checklist, Control 1	279
Table C-2	IG1 checklist, Control 2	279
Table C-3	IG1 checklist, Control 3	279
Table C-4	IG1 checklist, Control 4	279
Table C-5	IG1 checklist, Control 5	280
Table C-6	IG1 checklist, Control 6	280
Table C-7	IG1 checklist, Control 7	280
Table C-8	IG1 checklist, Control 8	280
Table C-9	IG1 checklist, Control 9	281
Table C-10	IG1 checklist, Control 10	281
Table C-11	IG1 checklist, Control 11	281

Table C-12	IG1 checklist, Control 12	281
Table C-13	IG1 checklist, Control 14	281
Table C-14	IG1 checklist, Control 15	282
Table C-15	IG1 checklist, Control 17	282
Table D-1	Worksheet header	283
Table D-2	Control 1: Inventory and Control of Enterprise Assets (5 Safeguards)	283
Table D-3	Control 2: Inventory and Control of Software Assets (7 Safeguards)	283
Table D-4	Control 3: Data Protection (14 Safeguards)	283
Table D-5	Control 4: Secure Configuration of Enterprise Assets and Software (12 Safeguards)	284
Table D-6	Control 5: Account Management (6 Safeguards)	284
Table D-7	Control 6: Access Control Management (8 Safeguards)	285
Table D-8	Control 7: Continuous Vulnerability Management (7 Safeguards)	285
Table D-9	Control 8: Audit Log Management (12 Safeguards)	285
Table D-10	Control 9: Email and Web Browser Protections (7 Safeguards)	285
Table D-11	Control 10: Malware Defenses (7 Safeguards)	286
Table D-12	Control 11: Data Recovery (5 Safeguards)	286
Table D-13	Control 12: Network Infrastructure Management (8 Safeguards)	286
Table D-14	Control 13: Network Monitoring and Defense (11 Safeguards)	286
Table D-15	Control 14: Security Awareness and Skills Training (9 Safeguards)	287
Table D-16	Control 15: Service Provider Management (7 Safeguards)	287
Table D-17	Control 16: Application Software Security (14 Safeguards)	287
Table D-18	Control 17: Incident Response Management (9 Safeguards)	288
Table D-19	Control 18: Penetration Testing (5 Safeguards)	288
Table D-20	Worksheet summary (count of Safeguards by status within the target IG)	288
Table E-1	Gap register header	291
Table E-2	Gap register (one row per Safeguard gap within the target IG)	291
Table E-3	Worked example rows (fictional 600-employee Pune NBFC, target IG2)	291
Table E-4	12-month action plan by quarter	291
Table E-5	Quarterly progress review	292
Table F-1	CIS Controls v8.1 to ISO/IEC 27001:2022 Annex A and clauses (indicative Srida IT mapping)	293
Table F-2	Selected CIS v8.1 Safeguards to ISO/IEC 27001:2022 Annex A (indicative Srida IT mapping)	295
Table G-1	Indian instruments referred to in the matrix (general description only)	297
Table G-2	CIS Controls v8.1 against Indian regulatory themes (indicative; confirm each row against the current instrument)	298
Table H-1	WP-C05 header	300
Table H-2	Populations used in testing	300
Table H-3	WP-C05 tests TP-C05-01 to TP-C05-03 and TP-C05-14	301
Table H-4	WP-C05 tests TP-C05-04 and TP-C05-05	301
Table H-5	WP-C05 tests TP-C05-06 and TP-C05-07	302
Table H-6	WP-C05 tests TP-C05-08 and TP-C05-09	302
Table H-7	WP-C05 tests TP-C05-10 and TP-C05-11	302
Table H-8	WP-C05 tests TP-C05-12 and TP-C05-13	303
Table H-9	WP-C05 Safeguard evaluation summary	303
Table H-10	WP-C05 findings register	304
Table H-11	WP-C05 Control 5 conclusion	304
Table H-12	WP-C05 sign-off	305
Table I-1	Report header	306
Table I-2	Summary position (two to three sentences each)	306
Table I-3	Safeguard coverage trend (from Appendix D)	306
Table I-4	Control status by RAG rating	307
Table I-5	Top five open gaps in business terms (from Appendix E)	307

Table I-6 Operational indicators (choose five to eight and keep them stable between reports) 307
Table I-7 Significant incidents, regulatory notifications and audit findings this period 308
Table I-8 Regulatory and assurance commitments (see Appendix G) 308
Table I-9 Decisions requested from the board 308

List of Figures

No figures.

PART I

Foundations

What the CIS Critical Security Controls are and what changed in v8.1, how Controls, Safeguards, asset classes, security functions and Implementation Groups fit together, how the Controls relate to ISO/IEC 27001, NIST CSF 2.0 and Indian regulation, terminology, and how to use this manual.

CHAPTER 1

Introduction to the CIS Controls v8.1

The CIS Critical Security Controls are a short, prioritised list of defensive actions that an enterprise can take to make the most common attacks fail. They are maintained by the Center for Internet Security (CIS), a not-for-profit organisation in the United States, and are written by a volunteer community of practitioners drawn from industry, government and academia. Version 8.1, released in June 2024, contains 18 Controls broken down into 153 Safeguards. This manual explains each of them, shows how an Indian enterprise of any size can implement them, and sets out testing procedures an assessor can use to judge whether they work.

This chapter covers where the Controls came from, what changed in version 8 and again in version 8.1, what the Controls are and are not, and why they are worth adopting in India alongside the frameworks and regulations that Indian enterprises already face.

1.1 What the Controls are

Most security frameworks describe outcomes: "the organisation manages its assets", "access is controlled". The CIS Controls take a different approach. They describe specific, testable actions, each of which an engineer can implement and an assessor can verify. A Safeguard such as maintaining an inventory of software, or requiring multi-factor authentication for remote network access, is concrete enough that two independent people looking at the same environment should come to the same answer about whether it is in place.

Three features set the Controls apart from longer catalogues such as ISO/IEC 27002 or NIST SP 800-53:

- **Prioritisation.** The Safeguards are sorted into three Implementation Groups (IG1, IG2 and IG3). IG1, which CIS calls “essential cyber hygiene”, is the set every enterprise should have, regardless of size. An enterprise does not have to decide alone which of 153 actions to start with.
- **Threat-informed selection.** CIS has repeatedly tested the Controls against real attack data. Its Community Defense Model (CDM) maps the Safeguards against the techniques used in the most frequent attack types, such as ransomware, web-application hacking and insider misuse, and reports how much protection each Implementation Group provides.
- **Brevity.** Each Safeguard is one short statement with a title and a description. The whole set fits into a document that a small IT team can read in an afternoon.

The Controls are not a management system standard. They do not tell an enterprise how to set its risk appetite, run a management review or assign accountability to its board. That is the job of ISO/IEC 27001, the NIST Cybersecurity Framework and sector regulation. The Controls fit underneath those frameworks as the technical and operational "how", and Chapter 4 shows how they connect.

> **No certification.** CIS does not certify organisations against the Controls, and no accredited scheme exists for doing so. An enterprise may assess itself, or engage an independent assessor, and report the result. It must not describe itself as certified. This manual is written for implementation and assessment, not for certification.

1.2 A short history

The Controls began in 2008 as an effort, led by US government agencies and private-sector security specialists, to answer one practical question: given limited budgets, which defensive actions stop the attacks that are actually happening? The answer was published as the Consensus Audit Guidelines and became widely known as the "SANS Top 20", because the SANS Institute hosted and promoted it.

Stewardship passed to the Council on CyberSecurity in 2013 and then to CIS in 2015, which has maintained the Controls since. Each new version has kept the original idea, a small number of prioritised and measurable actions, while updating the content for changes in technology and attack methods.

Table 1-1. Main versions of the CIS Controls

Version	Approximate date	What it introduced
Consensus Audit Guidelines / SANS Top 20	2008–2012	Twenty prioritised controls derived from observed attacks, with a strong emphasis on automation and measurement
Version 5 and Version 6	2014–2015	Transfer to the Council on CyberSecurity and then CIS; refined sub-controls; early mapping to the Verizon DBIR attack patterns
Version 7	March 2019	Twenty Controls arranged in Basic, Foundational and Organisational groups; clearer, single-action sub-controls
Version 7.1	April 2019	First Implementation Groups (IG1–IG3), replacing the idea that the first six Controls alone were "hygiene"
Version 8	May 2021	Consolidation to 18 Controls and 153 Safeguards; organised by activity rather than by who manages a device; cloud, remote working and service providers brought into scope
Version 8.1	June 2024	Govern security function; Documentation asset class; revised asset classes and glossary; clarified Safeguard descriptions; IG assignments unchanged

Why version 8 cut the list to eighteen

By version 7.1 the list described how a traditional, perimeter-based enterprise network was run: devices inside the office, managed by an IT department, protected by a firewall at the edge. That model no longer fitted most enterprises. Laptops worked from homes, applications ran in public cloud, and much of the processing was done by service providers the enterprise did not control.

Version 8 responded by grouping actions according to what is being done (inventory, configuration, access, monitoring) rather than where a device sits or who owns it. Several earlier Controls were merged. For example, separate Controls on wireless access, boundary defence and network ports were folded into the network infrastructure and network monitoring Controls. A new Control on service providers (Control 15) recognised that an enterprise's risk now depends heavily on outsourced IT, SaaS platforms and managed service providers. The sub-controls were renamed "Safeguards" to emphasise that each one is a concrete protective action.

What version 8.1 changed

Version 8.1 is an incremental release. CIS deliberately kept the 18 Controls, the 153 Safeguards and the Implementation Group of every Safeguard as they were, so that enterprises already using version 8 did not have to redo their work. The changes concern how the Safeguards are described and classified:

1. **A new Govern security function.** NIST added a Govern function when it published CSF 2.0 in February 2024. CIS followed, so that Safeguards that set direction, such as establishing a policy, maintaining a process, or reviewing a programme, are now labelled Govern rather than Identify or Protect. In v8.1, 25 of the 153 Safeguards carry the Govern function.
2. **A new Documentation asset class.** Policies, plans, processes and procedures are now treated as assets in their own right, with 20 Safeguards assigned to that class. This makes it easier to see which Safeguards an assessor tests by examining a document, as opposed to configuration or behaviour.
3. **Revised asset classes.** The asset classes were redefined and renamed, so that each Safeguard now points to one of six classes: Devices, Software, Data, Users, Network and Documentation. Chapter 2 explains each.
4. **An expanded glossary.** Words used with a specific meaning in the Safeguards, such as "plan", "process" and "sensitive data", now have published definitions.
5. **Clarified descriptions.** A number of Safeguard descriptions were reworded or expanded with examples, and minor errors were corrected, without changing what each Safeguard asks for.

For an enterprise already working to version 8, the practical effect is small: re-label Safeguards to the new function and asset class, review the reworded descriptions, and check that documentation-type Safeguards have owners and review dates. For an assessor, the Govern and Documentation labels are useful signposts, because they mark where a written artefact, approved and reviewed, is the primary evidence.

> **Later point releases.** CIS may publish minor corrections to v8.1 after June 2024. Readers should obtain the current version from the CIS website and check whether any Safeguard wording has been revised since this manual was prepared.

1.3 The 18 Controls at a glance

The table below lists the Controls with the number of Safeguards each contains, taken from the v8.1 data used to build this manual. The numbering is not a strict order of priority; prioritisation comes from the Implementation Groups, discussed in Chapter 3.

Table 1-2. The 18 CIS Controls v8.1 and their Safeguard counts

No.	Control	Safeguards	Of which IG1
1	Inventory and Control of Enterprise Assets	5	2
2	Inventory and Control of Software Assets	7	3
3	Data Protection	14	6
4	Secure Configuration of Enterprise Assets and Software	12	7
5	Account Management	6	4
6	Access Control Management	8	5
7	Continuous Vulnerability Management	7	4
8	Audit Log Management	12	3
9	Email and Web Browser Protections	7	2
10	Malware Defenses	7	3
11	Data Recovery	5	4
12	Network Infrastructure Management	8	1
13	Network Monitoring and Defense	11	0
14	Security Awareness and Skills Training	9	8
15	Service Provider Management	7	1
16	Application Software Security	14	0
17	Incident Response Management	9	3
18	Penetration Testing	5	0
	Total	**153**	**56**

Two patterns stand out. First, IG1 is heavily weighted towards the "know what you have, configure it safely, control who can use it, and be able to recover" Controls: 1 to 7, 11 and 14. Second, three Controls (13, 16 and 18) have no IG1 Safeguards at all. Network monitoring, secure software development and penetration testing need skills and tooling that a small enterprise normally does not have, and CIS has judged that a small enterprise gets more protection from finishing IG1 first.

1.4 Why the Controls suit Indian enterprises

Indian enterprises face a growing set of cyber security obligations: the CERT-In Directions of April 2022 on incident reporting and log retention, sector rules from RBI, SEBI and IRDAI, and, since 2023, the Digital Personal Data Protection Act with its duty to take reasonable security safeguards. These instruments generally say *what* must be achieved (protect personal data, report incidents quickly, keep logs) without saying in detail *how*. The CIS Controls supply a practical "how" that is recognised internationally and that an assessor can test.

The Controls also suit the shape of the Indian economy. A large share of Indian businesses are micro, small and medium enterprises with no dedicated security staff. IG1 was designed for exactly that kind of organisation: a 40-person chartered accountancy firm in Kochi or a family-run textile exporter in Coimbatore can implement most of IG1 with built-in operating system features, a reputable endpoint protection product, cloud backups and some discipline. At the other end, a Pune NBFC or a Bengaluru SaaS company serving overseas clients can use IG2 and IG3 to structure a mature programme and to answer customer security questionnaires, many of which ask about the CIS Controls directly.

Finally, the Controls are free to use for internal purposes. An enterprise can download them, implement them and assess against them without paying a licence fee, subject to the CC BY-NC-ND 4.0 licence terms described in Chapter 6.

1.5 What adopting the Controls looks like

Adopting the Controls is a programme, not a project. A typical sequence, expanded in Part III, is:

1. Decide the scope: which entities, sites, cloud tenants and services are covered.
2. Choose a target Implementation Group, using the factors in Chapter 3.
3. Assess the current state against that IG, Safeguard by Safeguard, using the procedures in Part II.
4. Prioritise gaps, starting with IG1 Safeguards that are not implemented, and build a dated action plan.
5. Implement, document and assign owners, with policies and procedures recorded where a Safeguard asks for them.
6. Measure, using the metrics proposed in each Control chapter, and reassess at least annually.

Many enterprises already hold ISO/IEC 27001 certification or report to a regulator. For them, the Controls are best treated as a technical baseline inside the existing management system, with the crosswalks in Chapter 4 and Appendix F used to avoid duplicated effort.

1.6 Supporting resources from CIS

CIS publishes a range of material around the Controls. The following may help readers, but availability, names and terms change, so each should be checked on the CIS website before use:

- the CIS Controls Self Assessment Tool (CSAT), for recording and tracking an enterprise's own implementation status;
- CIS Benchmarks, configuration guides for specific operating systems, cloud platforms and applications, which support Control 4;
- the CIS Community Defense Model, whose v3.0 was published in September 2026, relating Safeguards to attack techniques;
- the CIS Controls Navigator, an online view of the Controls and their mappings to other frameworks;
- companion guides, for example on cloud, mobile and small business use, and on measurement.

This manual does not reproduce any of these resources and is not a substitute for them. It is an independent commentary written to help Indian practitioners implement and test the Controls.

CHAPTER 2

Structure: Controls, Safeguards, Asset Classes, Security Functions

Every Safeguard in the CIS Controls v8.1 carries four pieces of metadata besides its title and description: the Control it belongs to, the asset class it protects, the security function it performs, and the lowest Implementation Group in which it appears. Understanding these labels makes the Controls far easier to plan, implement and assess. This chapter explains each layer and shows how the 153 Safeguards are distributed across them. All counts are taken from the v8.1 canon used to build this manual.

2.1 Controls and Safeguards

A **Control** is a theme: a broad area of defensive practice such as account management or data recovery. The 18 Controls are numbered 1 to 18. CIS presents each Control with an overview of its purpose, an explanation of why it matters, notes on procedures and tools, and a table of Safeguards. This manual does not reproduce those sections; Part II gives its own commentary on each.

A **Safeguard** is a single action within a Control, numbered with the Control number and a sequence number, for example 5.3 or 16.11. Before version 8, Safeguards were called sub-controls. Each Safeguard is intended to be:

- **specific** enough that it is clear what has to be done;
- **measurable**, so that its presence and coverage can be shown with evidence; and
- **independent** as far as possible, so that it can be implemented and assessed on its own, even though in practice many Safeguards depend on others (for example, most of Control 4 depends on the inventories of Controls 1 and 2).

Safeguards vary in nature. Some require a document to exist and be kept current (a data management process, an incident response plan). Some require a technical configuration (automatic screen locking, encrypted storage on end-user devices). Some require an activity at a frequency (monthly review of accounts, quarterly vulnerability scanning). The assessment procedures in Part II reflect these differences: a document is examined, a configuration is inspected or re-performed, and a recurring activity is sampled over a period.

Reading a Safeguard's wording

Safeguard titles start with a verb that tells the reader what kind of obligation applies. "Establish and Maintain" appears frequently and means two things: the item must be created, and it must be kept up to date through periodic review. Where the description gives a review frequency, typically annually or "when significant enterprise changes occur", both triggers apply. An assessor should not accept a document that was written once and never reviewed. Other common verbs are "Use", "Configure", "Deploy", "Perform" and "Address", each of which implies operating evidence rather than a document alone.

2.2 Asset classes

Each Safeguard is linked to one asset class, which identifies what it protects or governs. Version 8.1 uses six classes. The definitions below are this manual's summaries; the authoritative definitions are in the CIS glossary.

Table 2-1. The six v8.1 asset classes

Asset class	What it covers (summary)	Typical sub-types	Safeguards
Devices	Physical, virtual and cloud-hosted hardware that stores or processes data, including items that connect remotely	End-user devices (desktops, laptops, phones, tablets), servers, network devices, IoT and non-computing devices, removable media	25
Software	Programs and code that run on devices	Operating systems, applications, services, libraries, APIs, firmware	24

Asset class	What it covers (summary)	Typical sub-types	Safeguards
Data	Information the enterprise holds, whether sensitive or not, and whether digital or on paper	Sensitive data, log data, physical data	33
Users	People and the accounts through which they and systems act	Workforce, service providers, user accounts, administrator accounts, service accounts	29
Network	Interconnected infrastructure and the way it is designed	Network infrastructure, network architecture	22
Documentation	Written governance material, physical or digital	Plans, policies, processes, procedures	20
	Total		**153**

Notes on the classes

Devices. Network devices such as firewalls and switches are managed like any other device (inventoried, configured, patched) and so sit under Devices for those purposes. Safeguards about how traffic flows through them sit under Network. Removable media counts as a device. Cloud virtual machines and containers count as devices if they store or process data.

Software. Firmware is software. So are browser extensions, scripts and third-party libraries. In SaaS-heavy environments, many "applications" are services consumed through a browser, and the enterprise's control over them is through configuration and accounts rather than installation.

Data. Log data is treated as data, which is why most of Control 8 (Audit Log Management) falls into this class: 11 of its 12 Safeguards. Paper records are data too, which matters for Indian enterprises that still hold large volumes of physical KYC files, patient records or statutory registers.

Users. The class covers both people (workforce and service providers) and accounts. Contractors usually form part of the workforce; consultants and service providers often do not, depending on the contract. Control 14 (training) and Control 5 (accounts) sit almost entirely here.

Network. This class includes the network architecture itself, so architecture diagrams are evidence for Network Safeguards as well as Documentation ones.

Documentation. New in v8.1. A Safeguard in this class is satisfied primarily by a written, approved and maintained artefact. CIS distinguishes four forms: a *policy* states objectives and what is required or forbidden; a *plan* puts policies into effect and may bundle processes and procedures; a *process* is a set of general activities directed at a security goal; and a *procedure* is an ordered set of steps for a specific task. An assessor examining a Documentation Safeguard looks for content, approval, ownership, communication and review history.

Asset classes by Control

Most Controls are concentrated on one or two asset classes. The following table shows the distribution, which is useful for assigning ownership: the team that manages devices will own most of Controls 1, 4 and 10, while the identity team will own most of 5 and 6.

Table 2-2. Safeguards per Control by asset class (v8.1)

Control	Devices	Software	Data	Users	Network	Documentation	Total
1	5						5
2		7					7
3			14				14
4	7		2	1		2	12
5				6			6
6		1		5		2	8
7		5				2	7

Control	Devices	Software	Data	Users	Network	Documentation	Total
8			11			1	12
9	1	2			4		7
10	7						7
11			4			1	5
12	2				5	1	8
13	3				8		11
14				8		1	9
15			2	3		2	7
16		9		1	1	3	14
17				5		4	9
18					4	1	5
Total	**25**	**24**	**33**	**29**	**22**	**20**	**153**

2.3 Security functions

Each Safeguard is also labelled with one security function. In v8.1 these follow the six Functions of NIST CSF 2.0, which makes it straightforward to present CIS-based work to a board or regulator that thinks in CSF terms. The function describes the purpose of the action in the life cycle of defence: setting direction, knowing the estate, preventing harm, noticing problems, reacting, and restoring.

Table 2-3. The six security functions and their Safeguard counts (v8.1)

Function	Purpose in this manual's words	Safeguards	Examples
Govern	Set and maintain the direction, policy, roles and oversight for a security activity	25	3.1, 4.1, 6.1, 7.1, 15.2, 17.4
Identify	Know what assets, data, software and weaknesses exist	15	1.1, 2.1, 3.2, 5.1, 7.5
Protect	Prevent or limit harm through configuration, access restriction, encryption and training	78	4.3, 5.2, 6.3, 10.2, 14.2
Detect	Notice unauthorised assets, malicious activity or control failure	23	1.3, 8.2, 10.7, 13.1
Respond	Act on what has been detected to contain or remove it	6	1.2, 2.3, 7.7, 17.1
Recover	Restore data and services after an incident	6	11.2, 11.4, 17.8
	Total	**153**	

Protect dominates, with just over half of all Safeguards. That reflects the Controls' purpose: they are a defensive baseline, and most defensive actions prevent rather than detect. Respond and Recover have only six Safeguards each, because detailed incident handling and business continuity are left to Control 17 and to other frameworks. Enterprises that need deeper coverage of response and recovery, such as regulated financial entities, will normally supplement the Controls with sector requirements.

The Govern function in practice

The 25 Govern Safeguards are spread over 13 Controls. They are the places where an enterprise must decide, write down and periodically revisit how it intends to operate: the data management process (3.1), the secure configuration process (4.1 and 4.2), the access granting and revoking processes (6.1, 6.2), the vulnerability and remediation processes (7.1, 7.2), the audit log process (8.1), the recovery process (11.1), the service provider policy and related Safeguards (15.2–15.6), and the incident contact details, reporting process and response process (17.2–17.4), among others. Control 15 is the most governance-heavy, with five of its seven Safeguards labelled Govern.

For an assessor, Govern Safeguards answer the question "is there an intended design?" before operating Safeguards answer "does it work?". A missing Govern artefact usually explains why related operating Safeguards are inconsistent: if there is no documented process for granting access (6.1), it is unlikely that every new joiner received the same approvals.

Functions by Control

Table 2-4. Safeguards per Control by security function (v8.1)

Control	Govern	Identify	Protect	Detect	Respond	Recover
1		2		2	1	
2		2	3	1	1	
3	1	3	9	1		
4	2		10			
5	1	2	3			
6	3	1	4			
7	2	2	2		1	
8	1		3	8		
9			7			
10			4	3		
11	1		1			3
12	1		7			
13			6	5		
14	1		8			
15	5	1	1			
16	3	2	8	1		
17	3				3	3
18	1		2	2		
Total	**25**	**15**	**78**	**23**	**6**	**6**

Asset class against function

Crossing the two labels shows where each kind of work falls. Documentation Safeguards are almost entirely Govern (19 of 20; the other is Recover). Network Safeguards are all Protect or Detect. Data carries the largest share of Detect Safeguards because of the log management work in Control 8.

Table 2-5. Asset class by security function (v8.1)

Asset class	Govern	Identify	Protect	Detect	Respond	Recover	Total
Devices	0	2	16	6	1	0	25
Software	0	7	13	2	2	0	24
Data	2	3	16	9	0	3	33
Users	4	3	17	0	3	2	29
Network	0	0	16	6	0	0	22
Documentation	19	0	0	0	0	1	20
Total	**25**	**15**	**78**	**23**	**6**	**6**	**153**

2.4 Implementation Group labels

The fourth label is the lowest Implementation Group in which the Safeguard applies: IG1, IG2 or IG3. Because the groups are cumulative, a Safeguard labelled IG1 applies to every enterprise, one labelled IG2 applies to IG2 and IG3 enterprises, and one labelled IG3 applies only to IG3 enterprises. Of the 153 Safeguards, 56 are IG1, 74 are first introduced at IG2 (making 130 in total for an IG2 enterprise) and 23 are first introduced at IG3 (making all 153). Chapter 3 discusses the groups in depth.

2.5 How the labels are used in this manual

- The build prints each Safeguard's title, asset class, function and IG directly from the canon data, so these labels are always exactly as CIS published them. Nothing in this manual reassigns a Safeguard to a different class, function or group.
- The Control chapters in Part II use the function label to shape test design: Govern and Documentation Safeguards are tested mainly by examination and interview; Protect Safeguards by inspection and re-performance; Detect and Respond Safeguards by sampling alerts, tickets and logs over the period.
- Appendix A, the Safeguard Matrix, lists all 153 Safeguards with their labels so that readers can filter by any combination.
- The asset class tables in this chapter can be used directly to allocate Control ownership in a RACI.

> **Labels are aids, not rules.** The asset class and function labels help organise work, but they do not narrow a Safeguard's scope. A Safeguard labelled Devices may still require a documented procedure, and one labelled Documentation will usually have operational consequences that an assessor should sample. Read the Safeguard as a whole.

CHAPTER 3

Implementation Groups in Depth: Choosing Your IG

The Implementation Groups are the mechanism by which the CIS Controls prioritise. Rather than asking every enterprise to implement all 153 Safeguards, CIS sorts them into three cumulative groups and invites each enterprise to identify the group that best matches its circumstances. This chapter explains what each group contains, how the Safeguards are spread across the groups, how to choose a target group, and the mistakes to avoid. The CIS guide describes the typical enterprise for each group; readers should consult that description. What follows is this manual's own analysis and advice.

3.1 The three groups in outline

The groups are **cumulative**. An IG2 enterprise implements every IG1 Safeguard and the IG2 additions; an IG3 enterprise implements all 153. No Safeguard is ever dropped as an enterprise moves up.

Table 3-1. Safeguards in each Implementation Group (v8.1)

Group	New Safeguards at this level	Cumulative total	Share of all 153
IG1	56	56	37%
IG2	74	130	85%
IG3	23	153	100%

IG1: the floor for everyone

CIS describes IG1 as “essential cyber hygiene”. It is the minimum standard of information security for every enterprise, whatever its size or sector. It is not a "small company" option; a large bank that has not achieved IG1 has a basic hygiene problem, however advanced its other capabilities.

The 56 IG1 Safeguards are chosen to be achievable by an organisation with limited security skills, often using features already built into common operating systems, office suites and cloud platforms, and to stop the opportunistic, untargeted attacks that cause most incidents: commodity ransomware, credential stuffing, phishing, exploitation of unpatched internet-facing systems. In practice IG1 asks an enterprise to:

- know what devices, software, data, accounts and service providers it has (1.1, 2.1, 3.2, 5.1, 15.1);
- deal with anything unauthorised or unsupported (1.2, 2.2, 2.3);
- configure systems securely, with firewalls, session locks and managed default accounts (4.1–4.7);
- control access with unique passwords, separate administrator accounts, prompt removal of dormant and leavers' accounts, and MFA for internet-facing applications, remote access and administration (5.2–5.4, 6.1–6.5);
- patch operating systems and applications automatically, under a written process (7.1–7.4);
- collect and store basic audit logs (8.1–8.3);
- protect email and browsing, run anti-malware and stop removable media running automatically (9.1, 9.2, 10.1–10.3);
- back up data automatically, protect the backups and keep one copy isolated (11.1–11.4);
- keep network equipment current (12.1);
- train the workforce on the main risks (14.1–14.8); and
- know who handles incidents and how they are reported (17.1–17.3).

A 40-person chartered accountancy firm in Kochi can implement nearly all of this with a cloud productivity suite (with MFA and conditional access enabled), managed laptops with built-in disk encryption and firewall, an endpoint protection product, a DNS filtering service, automated cloud backups with an immutable or offline copy, a spreadsheet inventory reviewed every six months, and an annual awareness session supplemented by short phishing reminders.

IG2: managing complexity and sensitive data

IG2 adds 74 Safeguards. They are aimed at enterprises that have dedicated IT staff, several business units with different risk profiles, sensitive customer or regulated data, and a reputation that would suffer from a breach. The additions fall into recognisable themes:

- **Automation of discovery and inventory**: active discovery, DHCP logging, automated software inventory (1.3, 1.4, 2.4).
- **Allowlisting** of software and libraries (2.5, 2.6).
- **Deeper data protection**: classification, data flows, encryption at rest, in transit and on removable media, and segmentation by sensitivity (3.7–3.12).
- **Centralisation** of accounts, access control and network authentication (5.6, 6.7, 12.5).
- **Vulnerability scanning** of internal and external assets and tracked remediation (7.5–7.7).
- **Detailed and centralised logging** with time synchronisation, retention and review (8.4–8.11).
- **Network architecture and monitoring**: secure architecture, diagrams, VPN and AAA for remote devices, central alerting, host and network intrusion detection, segment filtering and flow logs (12.2–12.7, 13.1–13.6).
- **Programmes** for service provider management, secure development and penetration testing (15.2–15.4, 16.1–16.11, 18.1–18.3).
- **A full incident response capability**, with roles, communications, exercises and post-incident reviews (17.4–17.8).

IG2 is where most of the cost of a security programme sits: 74 Safeguards, many of which need enterprise-grade tooling (a SIEM, a vulnerability scanner, MDM, a central identity provider) and people who know how to run it.

IG3: resisting capable adversaries

IG3 adds the final 23 Safeguards. They address targeted attacks by skilled adversaries, insider misuse and the need to limit damage when a previously unknown vulnerability is exploited. They include passive asset discovery (1.5), script allowlisting (2.7), data loss prevention and logging of sensitive data access (3.13, 3.14), separated work profiles on mobile devices (4.12), role-based access control (6.8), collection of service provider logs (8.12), dedicated administrative workstations (12.8), intrusion prevention, port-level access control, application-layer filtering and alert tuning (13.7–13.11), assessment, monitoring and secure exit of service providers (15.5–15.7), code-level checks, application penetration testing and threat modelling (16.12–16.14), incident thresholds (17.9), and internal penetration testing with validation of security measures (18.4, 18.5).

IG3 needs specialist staff, for example application security engineers, threat hunters and red-teamers, or an equivalent managed service with genuine expertise.

3.2 How the groups are distributed across the Controls

The table below shows, for each Control, how many Safeguards apply at each group (cumulatively). It is the single most useful planning table in this manual: it tells an IG1 enterprise which Controls it can largely ignore for now, and an IG2 enterprise where the bulk of its additional work lies.

Table 3-2. Safeguards per Control applicable at each IG (cumulative, v8.1)

Control	IG1	IG2 (cumulative)	IG3 (all)	New at IG2	New at IG3
1 Enterprise assets	2	4	5	2	1
2 Software assets	3	6	7	3	1
3 Data protection	6	12	14	6	2
4 Secure configuration	7	11	12	4	1
5 Account management	4	6	6	2	0
6 Access control	5	7	8	2	1
7 Vulnerability management	4	7	7	3	0
8 Audit logs	3	11	12	8	1
9 Email and browser	2	6	7	4	1

Control	IG1	IG2 (cumulative)	IG3 (all)	New at IG2	New at IG3
10 Malware defences	3	7	7	4	0
11 Data recovery	4	5	5	1	0
12 Network infrastructure	1	7	8	6	1
13 Network monitoring	0	6	11	6	5
14 Awareness and training	8	9	9	1	0
15 Service providers	1	4	7	3	3
16 Application security	0	11	14	11	3
17 Incident response	3	8	9	5	1
18 Penetration testing	0	3	5	3	2
Total	**56**	**130**	**153**	**74**	**23**

Observations that shape planning:

- Fifteen of the 18 Controls have at least one IG1 Safeguard. Controls 13, 16 and 18 begin only at IG2.
- Six Controls (5, 7, 10, 11, 14 and, at IG2, nearly all of 4) are complete or almost complete by IG2. An IG2 enterprise that falls short in these has no "it is an IG3 item" excuse.
- The heaviest IG2 lifts are Control 16 (11 new Safeguards), Control 8 (8), and Controls 3 and 12 (6 each). An IG2 programme should budget for these.
- IG3 is concentrated in Control 13 (5 new) and Controls 15 and 16 (3 each).

Groups by function and asset class

Table 3-3. New Safeguards at each IG by security function (v8.1)

Function	IG1	New at IG2	New at IG3	Total
Govern	12	10	3	25
Identify	6	9	0	15
Protect	31	34	13	78
Detect	2	15	6	23
Respond	3	3	0	6
Recover	2	3	1	6
Total	**56**	**74**	**23**	**153**

IG1 is largely preventive and governance-led: 31 Protect and 12 Govern Safeguards out of 56, with only two Detect Safeguards (8.2 and 10.1). That is deliberate. A small enterprise cannot staff a monitoring function, so IG1 relies on preventing compromise and being able to restore. Detection capability arrives mainly at IG2, which adds 15 Detect Safeguards.

Table 3-4. New Safeguards at each IG by asset class (v8.1)

Asset class	IG1	New at IG2	New at IG3	Total
Devices	10	12	3	25
Software	6	14	4	24
Data	11	16	6	33
Users	17	10	2	29
Network	1	14	7	22
Documentation	11	8	1	20

Asset class	IG1	New at IG2	New at IG3	Total
Total	**56**	**74**	**23**	**153**

Users dominate IG1 (17 of 56), because people and accounts are where most opportunistic attacks start. Network Safeguards are almost absent from IG1 (only 12.1), reflecting the reality that many small enterprises have a single router and depend on cloud services.

3.3 Choosing a target IG

CIS leaves the choice of group to the enterprise. The decision should be documented, approved by management and revisited when the business changes. The following factors, weighed together, usually point clearly to one group.

Table 3-5. Factors for choosing a target Implementation Group (Srida IT guidance)

Factor	Points to IG1	Points to IG2	Points to IG3
Security and IT staffing	No dedicated staff; IT outsourced or handled part-time	An IT team, perhaps one or two security people	A security team with specialists, or a capable managed SOC
Data held	Mainly employee and routine business data	Customer personal data, financial or health data, client confidential data	Large volumes of sensitive personal data, payment data, critical national or public-service data
Regulatory exposure	General law only (IT Act, DPDP Act)	Sector rules apply to part of the business, or contractual security obligations to clients	Directly regulated as a bank, market infrastructure, insurer, critical information infrastructure or large data fiduciary
Tolerance for downtime	Business can work manually for a few days	Short interruptions acceptable; longer ones damage customers	Even brief outages cause public, financial or safety harm
Likely adversary	Opportunistic criminals	Criminals who select targets for value; insiders	Organised and well-resourced groups, including state-linked actors
Software development	None, or configuring SaaS only	Builds and runs its own applications	Applications are the product, or are used by the public at scale

Practical rules

1. **Start with IG1 regardless.** Even an enterprise whose profile points to IG3 should assess IG1 first and close IG1 gaps before investing in IG2 or IG3 Safeguards. An intrusion prevention system is of little value if administrator accounts have no MFA.
2. **Choose by the most demanding part of the scope, or split the scope.** A Hyderabad hospital chain may need IG3 rigour for its clinical systems and patient data but IG2 for its pharmacy retail outlets. Either set IG3 for the whole enterprise, or define separate scopes with separate targets and state this explicitly.
3. **Allow for clients' expectations.** A Bengaluru SaaS start-up with 60 staff may have an IG1 profile internally, but its enterprise customers in the US and Europe will expect IG2-level controls over the product environment, particularly Controls 8, 13 and 16.
4. **Regulation sets a floor, not the target.** If a regulator requires something that sits in IG3 (for example data loss prevention or specific monitoring), implement it, but that does not by itself make the enterprise IG3. Record it as an additional Safeguard implemented above the target group.
5. **Record the decision.** Write down the chosen group, the reasons, the scope, the approver and the next review date. An assessor will ask for it.

Indian examples

Table 3-6. Illustrative IG choices for fictional Indian enterprises

Enterprise	Profile	Suggested target

Enterprise	Profile	Suggested target
A 40-person Kochi CA firm	Client financial data, no IT staff, cloud email and files, outsourced support	IG1, plus 3.11 (encryption at rest) because of client confidentiality
A 300-employee Coimbatore textile exporter	ERP on-premises, small IT team, export buyers asking for security assurance	IG1 now, IG2 within 24 months for ERP and email
A Bengaluru SaaS start-up	Multi-tenant product in public cloud, handles customer personal data	IG2 for the product and corporate environments
A Chennai auto-parts maker with OT	Plant networks with PLCs and SCADA, corporate IT, tier-1 supplier to OEMs	IG2 for IT; IG2 for OT with network Safeguards prioritised and OT-specific guidance added
A 600-employee Pune NBFC	RBI-regulated, loan and KYC data, digital lending app	IG2 at minimum; IG3 for selected Safeguards required by the regulator
A Hyderabad hospital chain	Patient records, connected medical devices, 24×7 operations	IG3 for clinical systems; IG2 elsewhere

3.4 Common misconceptions

"IG1, IG2 and IG3 are maturity levels"

They are not. An Implementation Group defines *which* Safeguards apply to an enterprise; it says nothing about *how well* they are run. An IG1 enterprise can run its 56 Safeguards in an optimised, measured and continuously improving way; an IG3 enterprise can have all 153 in place on paper but operate them inconsistently. This manual therefore keeps two separate dimensions:

- the **Implementation Group**, which sets scope; and
- the **Srida IT maturity indicators** (Initial, Defined, Managed, Optimised) in each Control chapter, which describe how well the Control is run.

Reports should never say "we are at IG2 maturity". They should say, for example, "target IG2; 118 of 130 applicable Safeguards implemented; Control 8 at Defined maturity".

"Moving up a group is a promotion"

Moving to a higher group is a response to a higher-risk profile, not an achievement. An enterprise should not adopt IG3 to impress customers if it cannot operate the additional Safeguards; poorly run IG3 controls can create false confidence and operational noise.

"IG1 is only for small companies"

IG1 applies to every enterprise. Large organisations frequently have IG1 gaps hidden behind sophisticated tooling: incomplete asset inventories, unmanaged legacy accounts, untested backups. Assessments of large enterprises should report IG1 results separately for exactly this reason.

"Safeguards outside the target group are irrelevant"

They are optional, not irrelevant. An IG1 enterprise that can cheaply implement an IG2 Safeguard, for example DMARC (9.5) through its email provider, should do so. This manual's assessment method records such Safeguards as "implemented above target" so that the effort is recognised.

3.5 Recording the IG decision

The target IG should be captured in a short, approved record containing:

- the scope (legal entities, locations, cloud tenants, business services);
- the target group for each scope, with reasons tied to the factors above;
- any additional Safeguards adopted above the target group, and why (regulation, contract, risk);

- any Safeguards judged not applicable, each with a justification (for example, no in-house software development for Control 16);
- the approving executive and date; and
- the review trigger: at least annually, and on events such as a new regulated activity, an acquisition, or a move into software development.

Chapter 30 explains how this record is used to set the denominator for scoring, and Appendix D provides a worksheet.

CHAPTER 4

The CIS Controls and Related Frameworks

Very few Indian enterprises adopt the CIS Controls in isolation. Most already work to ISO/IEC 27001, report to a sector regulator, or answer customer questionnaires framed around the NIST Cybersecurity Framework. The CIS Controls are most useful when they are positioned correctly among these: as the concrete technical and operational baseline that sits under a management system and helps meet regulatory expectations. This chapter explains how the Controls relate to ISO/IEC 27001:2022, NIST CSF 2.0 and the principal Indian instruments, and how to use the crosswalks in this manual.

> **Mapping is not compliance.** A crosswalk shows that two requirements deal with related subject matter. It does not show that meeting one satisfies the other. An enterprise that implements every Safeguard mapped to an ISO/IEC 27001 control has evidence towards that control, not proof of conformity. The same applies, more strongly, to Indian legal obligations. All crosswalks in this manual are Srida IT's own judgement unless stated otherwise. CIS publishes its own official mappings on its website, and readers who need an authoritative mapping should use those.

4.1 Three kinds of framework

Table 4-1. How the CIS Controls differ from related frameworks

Framework	Type	What it gives you	What it does not give you
CIS Controls v8.1	Prioritised technical and operational safeguards	Specific, testable actions sorted by priority (IG1–IG3)	A management system, risk method, board governance or certification
ISO/IEC 27001:2022	Certifiable management system standard	Requirements to run an ISMS (clauses 4–10) and a reference set of 93 controls (Annex A)	Detailed technical settings or a priority order among controls
NIST CSF 2.0	Outcome-based framework	Six Functions, 22 Categories and 106 Subcategories describing desired outcomes; Profiles and Tiers	Prescriptive actions or a conformity scheme
Indian regulation	Legal and supervisory obligations	Binding requirements for specific entities, often with deadlines and reporting duties	A complete security baseline; most instruments set principles and leave the "how" to the entity

The relationship is complementary. ISO/IEC 27001 answers "how do we manage security as a system?"; CSF 2.0 answers "what outcomes should we achieve?"; regulation answers "what must we do by law?"; the CIS Controls answer "what specific actions, in what order, will make us defensible?".

4.2 ISO/IEC 27001:2022

Where the Controls fit in an ISMS

ISO/IEC 27001 requires an organisation to assess information security risks, select controls to treat them, compare those controls with Annex A, and produce a Statement of Applicability (clause 6.1.3). It does not mandate any particular control source. The CIS Controls can therefore be used in three ways inside an ISMS:

1. as a **control set** referenced in the risk treatment plan, alongside or in place of the Annex A list, with Annex A used as the completeness check the standard requires;
2. as **implementation guidance** for Annex A technological controls, giving concrete content to controls such as 8.8 (management of technical vulnerabilities) or 8.15 (logging); and
3. as a **technical audit programme**, supplying testing procedures for internal audit under clause 9.2.

The CIS Controls do not replace the ISMS clauses. Context (clause 4), leadership (5), risk assessment and treatment (6 and 8), competence and awareness (7.2, 7.3), performance evaluation (9) and improvement (10) all have to be run separately.

Govern-function Safeguards in v8.1 touch some of these, for example 14.1 supports clause 7.3 and Annex A 6.3, but they do not cover them.

Control-level crosswalk

The table gives a Control-level view of the Annex A controls each CIS Control most closely supports. It is Srida IT's mapping. The Safeguard-level crosswalk is in each Control chapter (section D) and in Appendix F.

Table 4-2. CIS Controls v8.1 to ISO/IEC 27001:2022 Annex A (Srida IT Control-level mapping)

CIS Control	Principal Annex A controls
1 Enterprise assets	5.9 Inventory of information and other associated assets; 8.1 User endpoint devices
2 Software assets	5.9; 8.19 Installation of software on operational systems
3 Data protection	5.12 Classification; 5.13 Labelling; 5.14 Information transfer; 5.33 Protection of records; 5.34 Privacy and protection of PII; 7.10 Storage media; 8.10 Information deletion; 8.12 Data leakage prevention; 8.24 Use of cryptography
4 Secure configuration	8.9 Configuration management; 8.1; 7.9 Security of assets off-premises
5 Account management	5.16 Identity management; 5.17 Authentication information; 5.18 Access rights; 8.2 Privileged access rights
6 Access control	5.15 Access control; 5.18; 8.2; 8.3 Information access restriction; 8.5 Secure authentication
7 Vulnerability management	8.8 Management of technical vulnerabilities; 8.19
8 Audit logs	8.15 Logging; 8.16 Monitoring activities; 8.17 Clock synchronisation
9 Email and browser	8.23 Web filtering; 8.7 Protection against malware; 5.14
10 Malware defences	8.7 Protection against malware; 7.10
11 Data recovery	8.13 Information backup; 5.30 ICT readiness for business continuity
12 Network infrastructure	8.20 Networks security; 8.21 Security of network services; 8.22 Segregation of networks; 8.9
13 Network monitoring	8.16 Monitoring activities; 8.20; 8.22; 5.25 Assessment and decision on information security events
14 Awareness and training	6.3 Information security awareness, education and training; clause 7.2, 7.3
15 Service providers	5.19 Information security in supplier relationships; 5.20 Addressing information security within supplier agreements; 5.21 Managing information security in the ICT supply chain; 5.22 Monitoring, review and change management of supplier services; 5.23 Information security for use of cloud services
16 Application security	8.25 Secure development life cycle; 8.26 Application security requirements; 8.27 Secure system architecture and engineering principles; 8.28 Secure coding; 8.29 Security testing in development and acceptance; 8.30 Outsourced development; 8.31 Separation of development, test and production environments
17 Incident response	5.24 Information security incident management planning and preparation; 5.25; 5.26 Response to information security incidents; 5.27 Learning from information security incidents; 5.28 Collection of evidence; 6.8 Information security event reporting
18 Penetration testing	8.8; 8.29; 5.35 Independent review of information security

Some Annex A controls have little or no CIS counterpart: most of the organisational controls on policies, roles, threat intelligence and legal requirements (5.1–5.8, 5.31–5.32), the people controls on screening and employment terms (6.1, 6.2, 6.4–

6.6), and nearly all physical controls (7.1–7.8, 7.11–7.14). An ISMS that relies on the CIS Controls for its technical baseline must cover these separately.

4.3 NIST Cybersecurity Framework 2.0

The CIS Controls v8.1 were deliberately aligned with CSF 2.0: every Safeguard's security function is one of the six CSF Functions, Govern included. That alignment is at Function level. At Category and Subcategory level the relationship is many-to-many, and the authoritative mapping is the one CIS publishes.

A practical way to combine the two is to use CSF 2.0 for the board-level Profile (current and target outcomes, Tiers, and the governance Categories in GV) and the CIS Controls for the implementation plan and testing underneath it. The table gives Srida IT's Category-level orientation.

Table 4-3. CIS Controls v8.1 to NIST CSF 2.0 Categories (Srida IT orientation)

CIS Control	Main CSF 2.0 Categories
1, 2	ID.AM Asset Management
3	ID.AM; PR.DS Data Security
4	PR.PS Platform Security
5, 6	PR.AA Identity Management, Authentication, and Access Control
7	ID.RA Risk Assessment; PR.PS
8	PR.PS; DE.CM Continuous Monitoring; DE.AE Adverse Event Analysis
9, 10	PR.PS; DE.CM
11	PR.DS; RC.RP Incident Recovery Plan Execution
12	PR.IR Technology Infrastructure Resilience; PR.PS
13	DE.CM; DE.AE; PR.IR
14	PR.AT Awareness and Training
15	GV.SC Cybersecurity Supply Chain Risk Management
16	PR.PS; ID.RA
17	RS.MA Incident Management; RS.CO Incident Response Reporting and Communication; RC.RP; ID.IM Improvement
18	ID.RA; ID.IM

CSF 2.0 Categories with weak CIS coverage include GV.OC (organisational context), GV.RM (risk management strategy), GV.RR (roles and authorities, beyond incident roles), GV.PO (policy, beyond the specific Safeguard-level processes) and GV.OV (oversight). These are management outcomes; they come from the enterprise's governance arrangements, ISO/IEC 27001 clauses 4–6 and 9, or sector regulation. Readers using the sister Srida IT manual on NIST CSF 2.0 can combine the two directly: the CSF manual supplies the governance and Profile layer, this manual the Safeguard-level implementation and testing.

4.4 Indian regulation

Indian cyber security regulation is fragmented across a general law, a national CERT, sector regulators and a new data protection regime. None of them mandates the CIS Controls, and none should be described as "met" by implementing them. The Controls are nevertheless a strong practical basis for meeting many technical obligations, as the table shows. All descriptions are general and should be checked against the current text of each instrument.

Table 4-4. Principal Indian instruments and the CIS Controls they draw on most

Instrument	Applies to (in general)	Key technical expectations	Most relevant CIS Controls

Instrument	Applies to (in general)	Key technical expectations	Most relevant CIS Controls
CERT-In Directions under s.70B(6) of the IT Act, 28 April 2022	Service providers, intermediaries, data centres, body corporates and government organisations	Report specified incidents within 6 hours; retain ICT system logs for 180 days within India; synchronise clocks to NIC or NPL NTP servers; designate a point of contact	8 (logs, time sync, retention), 17 (reporting, contacts), 13 (detection)
SEBI Cybersecurity and Cyber Resilience Framework (CSCRF), August 2024	SEBI-regulated entities, tiered by category and size	Governance, asset inventory, vulnerability assessment and penetration testing, SOC, logging, incident response, cyber resilience and audits by CERT-In empanelled auditors	1, 2, 7, 8, 13, 17, 18, plus Govern Safeguards
RBI Master Direction on IT Governance, Risk, Controls and Assurance Practices (2023) and related cyber security directions	Banks, NBFCs and other regulated entities, as specified	IT and security governance, access control, patching, logging, SOC, vendor risk, business continuity and IS audit	4, 5, 6, 7, 8, 11, 15, 17
IRDAI Information and Cyber Security Guidelines (2023)	Insurers and insurance intermediaries	Information security policy, risk assessment, controls on assets, access, data and suppliers, incident reporting and audit	1, 3, 5, 6, 15, 17
Digital Personal Data Protection Act 2023, s.8(5), and DPDP Rules 2025, rules 6 and 7	Data fiduciaries processing digital personal data	Reasonable security safeguards to prevent personal data breaches, including encryption or similar measures, access control, logging and monitoring, backups and retention of logs; intimation of personal data breaches to the Board and affected principals	3, 5, 6, 8, 11, 15, 17
CERT-In empanelled audits	Entities required by a regulator or government to obtain a security audit from an empanelled auditor	Audit scope set by the requiring authority; often includes VAPT and configuration review	4, 7, 16, 18

Using the Controls to meet Indian obligations

Three practical points arise repeatedly:

- **Logs and time.** The CERT-In 180-day log retention and NTP requirements bite directly on Control 8. An IG1 enterprise under the Directions will need to go beyond the IG1 Safeguards, in particular to retain logs (8.10) and synchronise time (8.4), both IG2 Safeguards. This is a clear case of regulation pulling an IG2 Safeguard into an IG1 enterprise's scope.
- **Incident reporting.** Control 17's IG1 Safeguards (17.1–17.3) give the skeleton for the 6-hour CERT-In report and DPDP breach intimation, but the enterprise must add the specific triggers, formats, recipients and timelines in its incident procedure.
- **Reasonable security safeguards.** The DPDP Act does not define the safeguards in technical detail. A documented, assessed implementation of the relevant CIS Safeguards is good evidence that safeguards were considered and applied, but whether they are "reasonable" will depend on the nature and volume of the data and on how the Data Protection Board interprets the requirement.

Each Control chapter in Part II includes an India touchpoints section (F) listing two to four instruments relevant to that Control. Appendix G consolidates them into a matrix.

4.5 Other frameworks

Each Control chapter's section E also gives selected mappings to other frameworks where they help Indian readers. These include:

- **NIST SP 800-53 Rev. 5** control families (for example AC, AU, CM, IR, RA, SI), at family level only;

- **PCI DSS v4.0.1** requirements, for enterprises that store, process or transmit payment card data, at requirement level where the relationship is clear;
- **ISO/IEC 27701** and **ISO/IEC 27002:2022** where privacy or implementation guidance adds to the ISO/IEC 27001 crosswalk;
- **MITRE ATT&CK** techniques, mainly through the CIS Community Defense Model, which relates Safeguards to attack techniques.

4.6 Building one control set

An enterprise subject to several frameworks should not run several programmes. Chapter 28 describes a "one control set" approach in which the CIS Safeguards form the technical baseline, each Safeguard carries tags for the ISO/IEC 27001 controls, CSF Subcategories and Indian obligations it supports, and evidence is collected once and reused. The table below shows how a single piece of work is reused in that model.

Table 4-5. One activity, many frameworks: an example for Safeguard 11.4

Framework	How the same evidence is used
CIS Controls	Evidence that an isolated recovery copy exists and is maintained (Safeguard 11.4)
ISO/IEC 27001:2022	Evidence for Annex A 8.13 Information backup, recorded in the Statement of Applicability
NIST CSF 2.0	Evidence towards PR.DS (backups protected) and RC.RP outcomes in the Current Profile
DPDP Rules 2025	Part of the evidence that reasonable safeguards include measures for continued processing after compromise
RBI / SEBI	Supporting evidence for business continuity and cyber resilience requirements

The discipline that makes this work is consistency: one owner per Safeguard, one evidence repository, one assessment calendar, and crosswalk tags that are reviewed whenever a framework is revised.

CHAPTER 5

Terminology and Abbreviations

This chapter gives working definitions of the terms used in this manual. They are Srida IT's own plain-language explanations. Where a term is defined in the CIS Controls v8.1 glossary, the source column says "CIS glossary" and the definition here is a summary for convenience; the CIS wording prevails in case of doubt. Other terms are defined as they are used in assessment practice, in Indian instruments or in this manual. Spellings follow British/Indian English except where a CIS title uses American spelling, which is kept unchanged.

5.1 Terms

Table 5-1. Terms used in this manual

Term	Working definition	Source
Administrator account	An account with elevated privileges used to manage devices, domains, applications or security tools. Each should belong to one named person and be separate from that person's everyday account (Safeguard 5.4).	CIS glossary
Allowlist	A list of items (software, libraries, scripts, domains) that are permitted; anything not on the list is blocked by default.	Srida IT
Application	A program or group of programs running on an operating system or delivered as a service, for example a web, database, mobile or SaaS application.	CIS glossary
Application Programming Interface (API)	A defined interface through which software components exchange data or invoke functions.	CIS glossary
Asset class	One of the six categories (Devices, Software, Data, Users, Network, Documentation) to which every v8.1 Safeguard is assigned.	CIS
Assessment	A structured, evidence-based evaluation of whether Safeguards are implemented and operating for a defined scope and period. Not a certification.	Srida IT
Assessment period	The span of time over which operating effectiveness is tested, normally the twelve months before fieldwork; for a first assessment it may be shorter and must be stated.	Srida IT
Assessor	The person or team performing the assessment, internal or external, with enough independence from the activities assessed to give an objective view.	Srida IT
Audit log	A record of events generated by a system, application or device, such as logons, changes, errors and security alerts.	Srida IT
Authorised	Approved through the enterprise's documented process for the item in question (asset, software, account, service provider) and recorded as such.	Srida IT
Compensating measure	An alternative arrangement that achieves the intent of a Safeguard where the usual approach is impractical; it must be documented, approved and evidenced.	Srida IT
Condition (finding)	What the assessor found, stated as fact with references to evidence.	Audit practice
Control	One of the 18 high-level themes of the CIS Controls, each containing several Safeguards.	CIS
Criteria (finding)	The requirement against which a condition is judged: the Safeguard, the enterprise's own policy, or a cited obligation.	Audit practice
Crosswalk	A table recording which requirements in two frameworks address related subject matter. It shows relationship, not equivalence.	Srida IT
Data fiduciary	Under the DPDP Act 2023, the person who alone or with others decides the purpose and means of processing personal data.	DPDP Act

Term	Working definition	Source
Data principal	Under the DPDP Act 2023, the individual to whom personal data relates (including the parent or guardian of a child).	DPDP Act
Design effectiveness	Whether a Safeguard, as designed and documented, would meet its intent if operated as described.	Audit practice
Device	Hardware, physical, virtual or cloud-hosted, that can store or process data: end-user devices, servers, network devices, IoT and non-computing devices, and removable media.	CIS glossary
Documentation	As an asset class: plans, policies, processes, procedures, diagrams and similar written material, physical or digital.	CIS glossary
Dormant account	An account that has not been used for a defined period, which the enterprise sets (CIS suggests 45 days for 5.3).	Srida IT
Effect (finding)	The actual or potential consequence of the condition: the risk that results.	Audit practice
End-user device	A device used by a member of the workforce: desktops, laptops, tablets and phones. Portable and mobile devices are subsets.	CIS glossary
Enterprise asset	Any device with the potential to store or process data, in physical, virtual or cloud environments.	CIS glossary
Essential cyber hygiene	CIS's description of IG1: the minimum set of Safeguards every enterprise should implement.	CIS
Establish and maintain	Create the item and keep it current, reviewing it at the stated frequency and when significant changes occur.	Srida IT
Evidence	Information the assessor obtains to support a conclusion: documents, system output, records, observations and interview notes.	Audit practice
Externally-exposed	Reachable from the internet or another untrusted network, whether hosted on premises or in the cloud.	Srida IT
Firmware	Software held in a device's non-volatile memory that lets the hardware work; often updated separately from the operating system.	CIS glossary
Implementation Group (IG)	One of three cumulative sets of Safeguards (IG1 = 56, IG2 = 130, IG3 = 153) used to prioritise implementation according to an enterprise's risk profile and resources. Not a maturity level.	CIS
Implemented	Evaluation result: evidence shows the Safeguard is in place for the whole scope, as designed, and operating over the period.	Srida IT
Incident	An event that actually or potentially harms the confidentiality, integrity or availability of a system or data, or breaches security policy.	Srida IT
Incident threshold	A defined point at which an event or group of events is treated as an incident and triggers the response process (Safeguard 17.9).	Srida IT
IoT and non-computing device	A device with embedded sensors or software that is not a general-purpose computer, such as printers, cameras, building controllers and industrial control equipment.	CIS glossary
Isolated recovery data	A backup copy kept out of reach of the production environment, for example offline, air-gapped or in a separately administered and immutable store.	Srida IT
Library	Reusable pre-built code included by applications, such as an open-source package.	CIS glossary
Log data	Machine-generated records of events, including operating system, application, network, security tool and physical access logs.	CIS glossary
Maturity indicator	Srida IT's four-level description (Initial, Defined, Managed, Optimised) of how well a Control is run. Separate from Implementation Groups.	Srida IT
Mobile device	A small enterprise-issued device with built-in wireless capability, such as a phone or tablet.	CIS glossary

Term	Working definition	Source
Network architecture	The physical and logical design of a network: its segments, connections and data flows, usually shown in diagrams.	CIS glossary
Network device	Equipment that enables communication on a network, such as firewalls, routers, switches, access points and gateways, physical or virtual.	CIS glossary
Not applicable	Evaluation result: the Safeguard's subject does not exist in scope (for example no removable media in use), with a written justification the assessor has verified.	Srida IT
Not implemented	Evaluation result: the Safeguard is absent, or present for so little of the scope or period that it gives no meaningful protection.	Srida IT
Operating effectiveness	Whether a Safeguard actually worked as designed, consistently, throughout the assessment period.	Audit practice
Operating system	Software that manages a device's hardware and provides common services to applications, such as Windows, Linux, macOS, Android or iOS.	CIS glossary
Partially implemented	Evaluation result: the Safeguard exists but falls short in scope, design or consistency of operation.	Srida IT
Personal data breach	Under the DPDP Act 2023, unauthorised processing or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data that compromises its confidentiality, integrity or availability.	DPDP Act
Plan	A document that puts policies into effect and may contain processes and procedures, for example an incident response plan.	CIS glossary
Policy	A formal management statement of security objectives that requires or prohibits specified actions.	CIS glossary
Population	The complete set of items from which a sample is drawn, such as all leavers in the period or all critical vulnerabilities raised.	Audit practice
Portable device	An end-user device that can be carried and connects wirelessly, such as a laptop, phone or tablet.	CIS glossary
Procedure	A sequence of steps to carry out a specific task in a specific environment.	CIS glossary
Process	A documented set of general activities to achieve a security goal; it may be documented in a plan, policy or procedure, or less formally.	CIS glossary
Removable media	Storage that can be detached from a running system, such as USB drives, external disks, memory cards, optical discs and tapes.	CIS glossary
Safeguard	A single, specific, measurable action within a Control. Called a sub-control before version 8. There are 153 in v8.1.	CIS
Sample	A subset of a population selected for testing so that a conclusion can be drawn about the whole.	Audit practice
Scope	The entities, locations, environments, systems and services covered by an implementation or assessment.	Srida IT
Security function	One of the six labels (Govern, Identify, Protect, Detect, Respond, Recover) given to each v8.1 Safeguard, aligned with NIST CSF 2.0 Functions.	CIS
Sensitive data	Data that must be protected from unauthorised disclosure, alteration or loss because harm would follow, including personal data, financial data and confidential business information.	CIS glossary
Server	A device or workload providing services or data to others, including physical servers, virtual machines, containers and serverless functions.	CIS glossary
Service account	A non-human account used by an application, service or automated task, with a named owner and a defined purpose.	CIS glossary

Term	Working definition	Source
Service provider	An external organisation providing platforms, software or services, including MSPs, SaaS and cloud providers and IT consultants.	CIS glossary
Significant enterprise change	A change that could affect a Safeguard's design, such as a merger, a new site, a new regulated activity, a cloud migration or a major system replacement; it triggers review of documentation.	Srida IT
Software	Code and instructions run by devices: operating systems, applications, services, libraries, APIs and firmware.	CIS glossary
Supported software	Software for which the vendor or maintainer still provides security updates.	Srida IT
Target IG	The Implementation Group an enterprise has decided, with documented reasons, to implement for a given scope.	Srida IT
User account	A standard account with limited privileges used by a person for everyday work.	CIS glossary
Workforce	Employees and others engaged by the enterprise, on-site or remote, who have access to its systems; usually includes contractors.	CIS glossary
Workpaper	The assessor's record of the tests performed, evidence obtained and conclusions reached for a Control, referenced WP-Cnn in this manual.	Srida IT

5.2 Abbreviations

Table 5-2. Abbreviations used in this manual

Abbreviation	Expansion
AAA	Authentication, Authorisation and Accounting (Auditing)
API	Application Programming Interface
ATT&CK	MITRE Adversarial Tactics, Techniques and Common Knowledge
BYOD	Bring Your Own Device
CA	Chartered Accountant (in examples); Certificate Authority (in technical contexts)
CDM	CIS Community Defense Model
CERT-In	Indian Computer Emergency Response Team
CI/CD	Continuous Integration / Continuous Delivery
CII	Critical Information Infrastructure
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CSAT	CIS Controls Self Assessment Tool
CSCRF	Cybersecurity and Cyber Resilience Framework (SEBI)
CSF	NIST Cybersecurity Framework
CSPM	Cloud Security Posture Management
DAST	Dynamic Application Security Testing
DBIR	Verizon Data Breach Investigations Report
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail

Abbreviation	Expansion
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DPDP	Digital Personal Data Protection (Act 2023; Rules 2025)
DPO	Data Protection Officer
EDR / XDR	Endpoint Detection and Response / Extended Detection and Response
HIDS / HIPS	Host-based Intrusion Detection System / Prevention System
IaC	Infrastructure as Code
IAM	Identity and Access Management
IdP	Identity Provider
IG	Implementation Group
IoT	Internet of Things
IRDAI	Insurance Regulatory and Development Authority of India
ISMS	Information Security Management System
IT Act	Information Technology Act, 2000
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MSP / MSSP	Managed Service Provider / Managed Security Service Provider
NBFC	Non-Banking Financial Company
NIC	National Informatics Centre
NIDS / NIPS	Network-based Intrusion Detection System / Prevention System
NIST	US National Institute of Standards and Technology
NPL	National Physical Laboratory (India)
NTP	Network Time Protocol
OT	Operational Technology
PAM	Privileged Access Management
PII	Personally Identifiable Information
RACI	Responsible, Accountable, Consulted, Informed
RBAC	Role-Based Access Control
RBI	Reserve Bank of India
RPO / RTO	Recovery Point Objective / Recovery Time Objective
SaaS / IaaS / PaaS	Software / Infrastructure / Platform as a Service
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SCA	Software Composition Analysis
SEBI	Securities and Exchange Board of India
SIEM	Security Information and Event Management

Abbreviation	Expansion
SLA	Service Level Agreement
SME / MSME	Small and Medium Enterprise / Micro, Small and Medium Enterprise
SOC	Security Operations Centre
SoA	Statement of Applicability (ISO/IEC 27001)
SPF	Sender Policy Framework
SSO	Single Sign-On
TP	Testing Procedure (as in TP-C05-01)
VAPT	Vulnerability Assessment and Penetration Testing
VPN	Virtual Private Network
WP	Workpaper (as in WP-C05)

5.3 Conventions in wording

- **Capitalised terms.** "Control", "Safeguard", "Implementation Group" and the six security function names are capitalised when they refer to the CIS terms.
- **Safeguard references.** Safeguards are cited by number (for example 5.3). Where a title is given, it is CIS's exact title, which may use American spelling ("Defenses", "Behavior").
- **"Enterprise".** CIS uses "enterprise" for any organisation adopting the Controls; this manual does the same, and uses "organisation" interchangeably in narrative text.
- **"Must" and "should".** In this manual's own guidance, "must" indicates what an assessor will expect to see for a Safeguard to be rated Implemented; "should" indicates good practice. Neither creates a new CIS requirement.

CHAPTER 6

How to Use This Manual and the Assessment Method

This manual is written for three audiences: those who implement the CIS Controls (IT managers, security engineers, MSPs), those who assess them (internal auditors, independent assessors, second-line risk teams), and those who oversee them (CISOs, risk committees, boards). Each can use it differently. This chapter explains how the manual is organised, how each Control chapter is laid out, the assessment method behind the testing procedures, the evaluation scale, the sampling approach, the convention and the licence terms that govern use of the CIS Controls.

6.1 How the manual is organised

Table 6-1. Parts of this manual and who they serve

Part	Content	Most useful to
I Foundations (Chapters 1–6)	History, structure, Implementation Groups, related frameworks, terminology and method	Everyone; read first
II The 18 Controls (Chapters 7–24)	One chapter per Control, with implementation guidance and testing procedures for every Safeguard	Implementers and assessors
III Implementation (Chapters 25–29)	90-day IG1 roadmap, growing into IG2 and IG3, tooling and baselines, one control set, SMEs and MSPs	Implementers, CISOs, MSPs
IV Assessment (Chapters 30–32)	Running an assessment, techniques and evidence, findings and reporting	Assessors and auditors
V Appendices (A–K)	Safeguard matrix, summaries, IG1 checklist, worksheets, crosswalks, India matrix, worked workpaper, board template, references	All, as working tools

Suggested reading paths

- **A small enterprise starting out:** Chapters 1 and 3, then the IG1 checklist (Appendix C) and the 90-day roadmap (Chapter 25). Use the Part II chapters only for the IG1 Safeguards that turn out to be gaps.
- **An enterprise with an ISO/IEC 27001 ISMS:** Chapters 2 and 4, then Chapter 28 and Appendix F, to fold the Safeguards into the Statement of Applicability and the internal audit programme.
- **An assessor:** this chapter, then Part IV, then the Part II chapters for the Controls in scope. Appendix H shows a completed workpaper.
- **A board or risk committee:** Chapter 1, the IG discussion in Chapter 3, and the reporting template in Appendix I.

6.2 The Control chapter format

Each of Chapters 7 to 24 follows the same layout, so that a reader who knows one chapter can find their way in any other. The sections are lettered A to X. Sections A to F set out the Control and its relationships; G to M give implementation guidance; N to S are the assessment procedures; T to X cover findings, improvement and a worked example.

Table 6-2. Sections of each Control chapter

Section	Title	What it contains
A	Control Reference and Safeguards	The Control title and every Safeguard's ID, title, asset class, security function and lowest IG, printed exactly from the CIS v8.1 data
B	Safeguard Implementation Guidance	For each Safeguard, a plain-language summary of what it requires in practice, two to four implementation steps and the evidence that shows it is in place

Section	Title	What it contains
C	Implementation Group Expectations	What an IG1, IG2 and IG3 enterprise must do for this Control, naming the Safeguards each group adds
D	ISO/IEC 27001:2022 Crosswalk	Srida IT's Safeguard-to-Annex A (and, where relevant, clause) mapping
E	Other Framework Mappings	Selected mappings to NIST CSF 2.0, NIST SP 800-53 Rev. 5 families and others, marked where uncertain
F	India Regulatory Touchpoints	Two to four Indian obligations relevant to the Control, described generally and marked
G	Overview and Why It Matters	What the Control is about, the attacks it defeats, what goes wrong without it, and the Indian angle
H	Interpretation	How the Control should be read, including points commonly misunderstood
I	Applicability	How the Control applies to small firms, cloud and SaaS-heavy enterprises, OT environments and outsourced IT
J	Implementation Guidance	Control-level implementation steps in a sensible order
K	Tools and Automation	Vendor-neutral tool categories and how they help
L	Roles and Responsibilities	Who does what, in a form that can be copied into a RACI
M	Documentation and Records	The policies, procedures, registers and records the Control needs
N	Assessment Testing Procedures	Numbered testing procedures (TP-Cnn-nn), at least one per Safeguard, each with its method
O	Sampling Guidance	Populations, sample sizes and period coverage specific to the Control
P	Interview Questions	Questions by role, to test understanding and corroborate documents
Q	Technical and Process Verification	Hands-on checks the assessor performs or observes
R	Expected Evidence	A consolidated list of evidence to request
S	Evaluation Criteria	Indicators of Implemented, Partially implemented and Not implemented for the Control
T	Common Gaps and Findings	Typical findings written as Condition – Criteria – Effect
U	Remediation Guidance	How to close the typical gaps
V	Monitoring Metrics	Measurable indicators for ongoing oversight
W	Related Controls and Maturity Indicators	Dependencies on other Controls and Safeguards, and the Srida IT maturity indicators (Initial, Defined, Managed, Optimised)
X	Implementation Example and Workpaper	A fictional Indian scenario showing the Control in practice, and the workpaper reference (WP-Cnn)

6.3 The assessment method

The testing procedures in section N follow the "requirements and testing procedures" style familiar from payment card assessments: for each requirement there are explicit tests that say what the assessor does and what they should see. The method rests on five principles.

1. **Scope first.** Before testing, the assessor confirms the scope (entities, sites, cloud tenants, services), the target Implementation Group, any Safeguards adopted above target, and any claimed as not applicable (see Chapter 3). The applicable Safeguards form the denominator for scoring.
2. **Design, then operation.** Each Safeguard is tested first for design (is there a documented and adequate way of doing it, covering the whole scope?) and then for operation (did it actually happen, consistently, across the period?). A well-designed Safeguard that did not operate is not implemented; neither is one that operated by accident without a design.

3. **Evidence over assertion.** Interviews show understanding and point to evidence; they are never sufficient on their own. Every conclusion must trace to documents, system output, records or observation.
4. **Period, not point.** Where a Safeguard implies a frequency (monthly review, quarterly scanning, annual update), the assessor tests occurrences across the assessment period against that frequency, not a single instance chosen by the enterprise.
5. **Proportion.** The depth of testing matches the size and risk of the enterprise. A 40-person firm's IG1 assessment can be completed in two or three days; a regulated entity's IG3 assessment may take weeks.

Testing methods

Each procedure states one of six methods. Most Safeguards need more than one, so several procedures may test the same Safeguard.

Table 6-3. Testing methods used in this manual

Method	What the assessor does	Typical use
Examine	Reads and evaluates documents: policies, processes, plans, registers, reports	Govern and Documentation Safeguards; design effectiveness
Interview	Asks the people who own or operate the Safeguard how it works	Understanding, corroboration, identifying where evidence is held
Observe	Watches a process being performed or a control operating	Joiner–leaver processing, backup restoration, incident exercises
Inspect	Looks directly at system configuration, consoles or output	Encryption status, firewall rules, MFA policies, log settings
Re-perform	Independently repeats a control or check to see whether the same result is obtained	Reconciling an inventory to discovery output, re-running a scan, attempting a blocked action
Sample	Selects items from a population over the period and tests each	Account reviews, patch cycles, remediation tickets, training records

Assessment workflow

1. **Plan:** agree scope, target IG, period, team, independence and timetable; issue an evidence request list based on section R of each Control in scope.
2. **Understand:** walk through the environment, architecture diagrams and key processes; hold the section P interviews.
3. **Test:** perform the section N procedures and section Q verifications; record everything in the workpaper (WP-Cnn).
4. **Evaluate:** rate each applicable Safeguard on the scale below, using the section S criteria.
5. **Report:** write findings in Condition – Criteria – Effect form with a recommendation, agree factual accuracy with owners, and present results by Control and by IG (Chapter 32 and Appendix I).
6. **Follow up:** track remediation against the action plan and re-test closed findings.

6.4 The evaluation scale

Every applicable Safeguard receives one of four results. The scale is deliberately simple: it records whether the Safeguard is in place, not how mature it is. Maturity is recorded separately at Control level using the Srida IT indicators in section W.

Table 6-4. Safeguard evaluation scale

Result	Meaning	Typical evidence pattern
Implemented	The Safeguard is designed adequately, covers the whole scope and operated consistently throughout the assessment period.	Documented and approved where required; technical settings confirmed by inspection; samples across the period show no exceptions, or only isolated exceptions promptly corrected
Partially implemented	The Safeguard exists but falls short in one or more of design, coverage or consistency of operation.	Process exists but is not documented or reviewed; control applies to most but not all of scope; samples show recurring exceptions; started part-way through the period

Result	Meaning	Typical evidence pattern
Not implemented	The Safeguard is absent, or present so narrowly that it gives no meaningful protection.	No process, tool or record; or only a draft policy; or coverage limited to a pilot
Not applicable	The subject of the Safeguard does not exist in scope, and the assessor has verified this.	Written justification approved by management, corroborated by inspection (for example, no removable media enabled on any device; no in-house software development)

Rules for applying the scale

- **Not applicable is rare.** It must be justified by the absence of the subject, never by cost, difficulty or the target IG. Safeguards outside the target IG are not rated "Not applicable"; they are simply outside scope and are reported only if implemented above target.
- **Compensating measures.** Where the enterprise meets the intent of a Safeguard by an alternative means, the assessor may rate it Implemented or Partially implemented, provided the alternative is documented, approved and shown to work. The workpaper records the reasoning.
- **New Safeguards.** A Safeguard introduced part-way through the period is normally rated Partially implemented, with the start date stated, unless the period is redefined.
- **Dependence.** A Safeguard that depends on another (for example 7.3 patching depends on 2.1 software inventory to know what to patch) can still be rated Implemented on its own evidence, but the finding on the prerequisite should note the dependency.
- **No averaging upwards.** A Control cannot be reported as fully implemented if any of its applicable Safeguards is Partially or Not implemented.

Scoring

Results are reported as counts and percentages of applicable Safeguards, separately for each IG level, for example: "IG1: 50 of 56 applicable implemented, 4 partially, 2 not; IG2 additions: 51 of 74 implemented". A simple score counts Implemented as 1, Partially implemented as 0.5 and Not implemented as 0, divided by the number of applicable Safeguards. The score is a summary only; reports should always show the underlying counts and the specific gaps. Chapter 30 gives the detail.

6.5 The sampling approach

Where a Safeguard operates repeatedly, the assessor tests a sample of occurrences drawn from the whole assessment period. The table gives Srida IT's default minimum sample sizes. They are judgement-based, not statistical, and are intended to give reasonable confidence for an internal or independent assessment. Section O of each Control chapter adjusts them where needed.

Table 6-5. Default minimum sample sizes (Srida IT guidance)

Frequency of the activity or size of population	Minimum sample
Annual (or on significant change)	1 (the most recent occurrence), plus evidence of the previous one where available
Quarterly	2 quarters
Monthly	3 months, spread across the period
Weekly	5 weeks
Daily	15–20 days
Many times a day / event-driven, population under 50	5 items or 10%, whichever is greater
Event-driven, population 50–250	10–25 items
Event-driven, population over 250	25–40 items
Configuration of devices, population under 50	All, where tooling allows; otherwise 10 items

Frequency of the activity or size of population	Minimum sample
Configuration of devices, population over 50	Full tool-based report, plus manual inspection of 10–25 devices across types and locations

Sampling rules

- **The assessor selects.** Samples are chosen by the assessor from a complete population supplied by the enterprise, never chosen by the enterprise. The assessor first checks that the population is complete, for example by reconciling the leavers list to HR records.
- **Spread.** Samples cover the whole period, all relevant locations, all device or account types, and both in-house and out-sourced operation.
- **Risk weighting.** Higher-risk items (administrator accounts, internet-facing servers, critical vulnerabilities, key service providers) are over-represented.
- **Prefer full populations.** Where a tool can produce a complete report (for example, encryption status of every laptop from MDM), the assessor uses the full population and samples only to confirm that the tool's output is reliable.
- **Exceptions.** One exception in a small sample usually requires the sample to be extended. Repeated exceptions indicate Partially implemented at best. Every exception is recorded with its cause.
- **Small enterprises.** In a 40-person firm many populations are tiny; the assessor simply tests them all.

6.6 Edition caveat

This edition was prepared from the CIS Controls v8.1 guide and Safeguard data published by CIS in 2024, together with Srida IT's knowledge of related frameworks and Indian instruments. It did not check every external reference against its primary source. Where the manual states a fact that could have changed since publication, or that was not confirmed against the primary text, the statement should be confirmed against the current primary source. Typical examples are:

- clause, section or rule numbers and timelines in Indian regulations and directions;
- specific mapping identifiers in other frameworks where the relationship is a matter of judgement;
- historical dates and version details of the CIS Controls before v8.1;
- the current name, availability and terms of CIS resources such as CSAT, CIS Benchmarks, the Community Defense Model and the Controls Navigator; and
- the availability of features in categories of tool.

Such statements are believed correct but must be checked before they are relied on in a finding, a contract, a regulatory submission or advice. The manual never invents regulatory paragraph numbers, deadlines or official CIS mappings; where an identifier is not certain, the subject is named and the identifier is left for the reader to confirm.

6.7 What this manual is not

- It is not the CIS Controls. The authoritative text is CIS's own publication, which readers should obtain and keep at hand.
- It is not a certification scheme. CIS does not certify organisations against the Controls, and an assessment using this manual results in a report, not a certificate.
- It is not legal advice. India touchpoints are general descriptions; obligations should be confirmed with the current text of each instrument and, where needed, legal counsel.
- It does not recommend vendors. Tools are named by category; open-source examples are illustrations only.

6.8 Licence and attribution

CIS Controls. The CIS Critical Security Controls are © Center for Internet Security, Inc. (CIS). They are licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License (CC BY-NC-ND 4.0); licence deed `https://creativecommons.org/licenses/by-nc-nd/4.0/`. Under that licence the Controls may be shared for non-commercial purposes with attribution, but modified versions of the Controls may not be distributed, and commercial use requires CIS's permission.

What this manual reproduces. This manual quotes verbatim only the titles of the 18 Controls and the 153 Safeguards, with their published asset class, security function and Implementation Group labels, so that readers can identify each item exactly. All other text, including the Safeguard summaries, implementation guidance, testing procedures, crosswalks and examples, is Srida IT's own work, written in its own words. It is commentary on the Controls, not a modified version of them. Readers should consult CIS's text for the authoritative descriptions.

Latest version. The current CIS Controls and related resources are available from CIS at `https://www.cisecurity.org/controls/`. Readers should check there for any revision issued after this manual was prepared.

Free and non-commercial. This manual is published by Srida IT free of charge and on a non-commercial basis. It may not be sold.

No affiliation. Srida IT is independent of the Center for Internet Security. It is not affiliated with CIS, and CIS has not reviewed or endorsed this manual or Srida IT's services. "CIS", "CIS Controls", "CIS Critical Security Controls" and "CIS Benchmarks" are trademarks of the Center for Internet Security, Inc., used here only to identify the subject matter.

Other frameworks referred to in this manual (ISO/IEC 27001:2022, NIST CSF 2.0, NIST SP 800-53 and Indian legal instruments) are cited for reference only. Their titles and control identifiers are used to describe relationships; their text is not reproduced.

PART II

The 18 CIS Controls

All 18 Controls and 153 Safeguards of CIS Controls v8.1, Control by Control: Safeguard titles with asset type, security function and Implementation Group, practical implementation steps, IG expectations, ISO/IEC 27001:2022 and other mappings, Indian regulatory touchpoints and assessment testing procedures for every Safeguard.

CHAPTER 7 · CIS CONTROL 1

Inventory and Control of Enterprise Assets

CIS CONTROL 1 · 5 SAFEGUARDS · 2 IN IG1

Inventory and Control of Enterprise Assets

CIS Controls v8.1 · titles quoted verbatim | WP-C01

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 1 — Inventory and Control of Enterprise Assets

Control 1 asks a deceptively simple question: does the enterprise know every physical and virtual device that touches its data, and can it tell which ones belong? It covers laptops, desktops, phones and tablets, servers, network equipment, printers, cameras and other IoT, virtual machines and cloud instances, and personally owned devices that connect regularly. The Control has two halves. The first is knowing: building and keeping a register that is accurate, detailed and owned. The second is controlling: finding devices that are not in the register and dealing with them promptly. Everything else in the CIS Controls leans on this register. You cannot patch, harden, monitor, back up or encrypt a device you do not know exists, so the inventory is the denominator against which almost every other Safeguard is measured.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 7-1. Safeguards of CIS Control 1, Inventory and Control of Enterprise Assets

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
1.1	**“Establish and Maintain Detailed Enterprise Asset Inventory”**	Devices	Identify	**IG1**	Keep one authoritative, current register of every hardware asset that can hold or handle enterprise data, wherever it sits (office, home, data centre, cloud tenancy or plant floor), with enough identifying and ownership detail to tell an approved device from a stranger. The register is reviewed and corrected at least twice a year.
1.2	**“Address Unauthorized Assets”**	Devices	Respond	**IG1**	Run a defined routine, at least weekly, that takes every device found on the network but absent from the approved register and resolves it: approve and record it, isolate it, block its remote access, or physically remove it.
1.3	**“Utilize an Active Discovery Tool”**	Devices	Detect	**IG2**	Use a tool that actively probes the enterprise's network ranges to find connected devices, scheduled to run every day or more often, so that the register is checked against reality rather than memory.
1.4	**“Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory”**	Devices	Identify	**IG2**	Turn on logging on every DHCP server or IP address management platform and use those lease records, at least weekly, to spot new devices and keep the register's addressing and naming details current.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
1.5	**“Use a Passive Asset Discovery Tool”**	Devices	Detect	IG3	Deploy passive monitoring that watches network traffic to identify devices without sending probes, which suits sensitive segments and catches devices that dodge scans; use what it sees at least weekly to update the register.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
1.1	**1.** Define the minimum record for each asset: hostname, MAC address, IP address where fixed, asset owner, department, location, asset class, and an explicit approved / not-approved flag for network connection. **2.** Seed the register from every source you already have (purchase orders, fixed-asset ledger, MDM, directory computer objects, cloud console exports, switch ARP and MAC tables) and reconcile duplicates. **3.** Include virtual machines, cloud instances, network gear, printers, CCTV, biometric readers and other IoT, plus personally owned devices that regularly connect. **4.** Assign a register owner and a review calendar (at least half-yearly), and tie joiner, purchase, transfer and disposal events to register updates.	• Current asset register export with the mandatory fields populated • Records of the last two half-yearly reviews with changes made • Procedure linking procurement and disposal to register updates
1.2	**1.** Write a short procedure naming who reviews new or unknown devices each week and the permitted outcomes (register, quarantine, deny remote access, remove). **2.** Provide a technical means of isolation, such as a quarantine VLAN, switch-port shutdown, NAC rejection or a Wi-Fi block list. **3.** Record each unknown device as a ticket with discovery date, outcome and closure date, so the weekly cadence can be evidenced.	• Weekly unauthorised-device review records or tickets • Configuration showing quarantine or blocking capability • Sample of resolved unknown-device tickets
1.3	**1.** Select an active discovery capability (network scanner, the discovery module of a vulnerability scanner, or an asset-management agent with network sweep) and give it credentials only where needed. **2.** Define the scope as every in-use subnet, including Wi-Fi, VPN pools, branch and plant networks and cloud VPCs, and agree safe scan settings with OT owners before scanning plant networks. **3.** Schedule scans daily at minimum and feed results automatically into the register comparison used for 1.2.	• Scanner schedule and scope configuration • Daily scan run history for a sample period • Report showing discovered devices compared with the register
1.4	**1.** Enable DHCP audit logging on all servers, including firewalls and wireless controllers that hand out addresses at branches. **2.** Forward the logs to a central store or SIEM and keep them for the retention period your log policy requires. **3.** Build a weekly comparison of leased MAC addresses against the register and route unknown MACs into the 1.2 process.	• List of all DHCP sources with logging enabled • Sample DHCP logs in the central store • Weekly reconciliation output and resulting register changes

Safeguard	Practical steps	Evidence
1.5	1. Place passive sensors on SPAN ports or taps at core switches, internet edge and sensitive segments such as OT or payment networks. 2. Tune fingerprinting so that device type, vendor and protocol are recorded, and suppress known noise. 3. Review passive findings weekly against the register and the active-scan results, and treat any device seen only passively as a priority investigation.	• Sensor placement diagram • Weekly passive-discovery review records • Examples of register updates triggered by passive findings

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
An IG1 enterprise must keep a complete, owned asset register with the key identifying fields (1.1) and run a weekly routine to deal with devices that are not in it (1.2). A small firm can meet this with a well-kept spreadsheet or the asset module of its MDM or helpdesk tool, plus a weekly look at the router or Wi-Fi controller's client list. The test is not tooling but completeness, currency and evidence that unknown devices are actually handled.	IG2 adds automation so the register does not depend on people remembering: a daily active discovery scan across all network ranges (1.3) and use of DHCP or IPAM logs at least weekly to catch new devices and keep addressing current (1.4). Most IG2 organisations integrate these feeds with a CMDB or asset platform.	IG3 adds passive discovery (1.5), watching traffic to identify devices that do not answer probes or that appear only briefly. It is most relevant where active scanning is risky, such as OT and medical device networks, or where the threat model includes deliberate rogue devices.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 1.1 → 5.9 Inventory of information and other associated assets; 5.11 Return of assets; 8.1 User endpoint devices
- 1.2 → 5.9; 8.20 Networks security; 8.22 Segregation of networks (quarantine)
- 1.3 → 5.9; 8.16 Monitoring activities
- 1.4 → 5.9; 8.15 Logging
- 1.5 → 5.9; 8.16 Monitoring activities
- Control-level → clause 8.1 Operational planning and control; 7.9 Security of assets off-premises; 7.14 Secure disposal or re-use of equipment

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: ID.AM-01 (hardware inventories), ID.AM-08 (asset life-cycle management), DE.CM-01 (network monitoring) (Srida IT mapping)
- NIST SP 800-53 Rev. 5: CM-8 System Component Inventory; CM-8(3) automated unauthorised component detection; PM-5 System Inventory; SI-4 System Monitoring
- PCI DSS v4.0.1: Requirement 12.5.1 (inventory of in-scope system components) and 9.5.1 (POI device inventory) where card data is in scope

F India Regulatory Touchpoints

- CERT-In Directions (28 April 2022): incident reporting within six hours and log retention of 180 days presuppose a known set of log-producing assets
- SEBI CSCRF (2024): regulated entities are expected to maintain an inventory of IT and cyber assets, including those of third parties, and review it periodically
- RBI Master Direction on IT Governance, Risk, Controls and Assurance Practices (2023) for banks and NBFCs: maintenance of an IT asset inventory with classification
- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6: reasonable security safeguards for personal data begin with knowing which devices hold it

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Attackers routinely scan an organisation's address space looking for the forgotten machine: the test server stood up for a project and never decommissioned, the unmanaged NAS a department bought on a credit card, the CCTV recorder with a default password, the contractor laptop on guest Wi-Fi that was quietly moved to the office LAN. These devices are rarely patched or monitored, so they become the first foothold for ransomware operators and the quiet pivot point for lateral movement. Unknown devices also distort every security metric: a dashboard that reports 98% EDR coverage is meaningless if one in five devices is missing from the denominator.

Failure shows up after an incident. Responders cannot scope what was affected, insurers ask for the list of assets in the blast radius, and auditors find that the register used for ISO/IEC 27001 Annex A 5.9 was last updated a year ago. Recovery takes longer because nobody knows which systems need rebuilding or who owns them.

In India the pressure is concrete. The CERT-In Directions of April 2022 expect reportable incidents to be notified within a short window and logs to be available for a long retention period; neither is achievable without knowing which devices generate the logs. Regulated entities under SEBI's CSCRF and RBI's IT governance directions are expected to maintain asset inventories as a baseline control, and the DPDP Act's duty to protect personal data with reasonable safeguards starts with knowing which devices store it. Indian SMEs often run mixed estates with a high share of personal devices, branch offices on consumer-grade routers and outsourced IT, which makes an honest inventory both harder and more valuable.

I Applicability

Every enterprise, whatever its size, falls within this Control. A 40-person CA firm can satisfy IG1 with a spreadsheet kept up to date by its outsourced IT provider and a weekly check of the office Wi-Fi client list. Cloud- and SaaS-heavy organisations must remember that cloud instances, container hosts, managed databases and serverless endpoints are assets too; console or API exports usually give a better picture than network scans, and the register should record the cloud account and region. Organisations with OT (manufacturing, utilities, hospitals) must agree discovery methods with plant engineers, because aggressive active scans can crash PLCs and older medical devices; passive discovery and vendor-supplied asset lists are often the safer start. Where IT is outsourced to an MSP, the enterprise still owns the register: the contract should require the MSP to maintain it, share it on request and report unknown devices, and the enterprise should test that it does.

J Implementation Guidance

1. Appoint an owner for the asset register (often the IT manager or infrastructure lead) and agree the scope: all locations, home workers, cloud accounts, plant networks and third-party-managed devices.
2. Define the data model: mandatory fields, asset classes, criticality and the approved-to-connect flag. Keep it short enough to be maintained.
3. Build the first version by reconciling every existing source: finance asset ledger, purchase records, MDM, directory, EDR console, cloud inventories, switch tables and DHCP leases.
4. Link the register to life-cycle events: procurement, imaging and issue, transfer between users, repair, and disposal with certificate of destruction.
5. Introduce the weekly unknown-device routine with a defined set of outcomes and a technical way to isolate devices (quarantine VLAN, NAC or port shutdown).
6. At IG2, schedule daily active discovery across all ranges and integrate DHCP and IPAM logs, automating the comparison with the register.
7. At IG3, add passive sensors at key points, especially OT, payment and guest segments, and include their findings in the weekly review.
8. Hold a half-yearly full reconciliation and attestation by department heads, and report coverage metrics to management.
9. Use the register as the authoritative denominator for EDR, patching, backup and logging coverage reports under Controls 4, 7, 8, 10 and 11.

K Tools and Automation

- CMDB or IT asset management platform: holds the authoritative register, relationships and ownership, and supports reconciliation from multiple feeds.
- MDM / unified endpoint management: provides near-real-time records for laptops and mobile devices, including off-network and home-worker devices.

- Active network discovery or vulnerability scanner (for example, open-source Nmap or OpenVAS/Greenbone): sweeps subnets daily and fingerprints devices.
- DHCP / IPAM with log forwarding to a SIEM (for example, Wazuh): records every lease and supports weekly reconciliation.
- Network access control (NAC) and 802.1X: blocks or quarantines devices that are not approved, giving 1.2 its technical teeth.
- Passive network monitoring / OT asset visibility sensors: fingerprint devices from traffic without probing fragile equipment.
- Cloud security posture or cloud inventory tooling: lists instances and services across cloud accounts via API.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
IT / infrastructure manager	Owns the asset register, the discovery tooling and the weekly unknown-device review.
CISO / information security lead	Sets inventory requirements, monitors coverage metrics and escalates persistent unknown devices.
Department heads / asset owners	Confirm the assets assigned to their teams at each half-yearly review and report changes.
Procurement and finance	Notify IT of purchases and disposals and reconcile the fixed-asset ledger with the register.
OT / plant engineering lead	Approves discovery methods for plant networks and maintains OT asset details.
MSP or outsourced IT provider	Maintains the register and discovery tools where contracted, and reports on them.

M Documentation and Records

- Asset management policy or standard defining scope, mandatory fields and review frequency
- Asset register (CMDB export or spreadsheet) with change history
- Procedure for handling unauthorised devices, including isolation options and approval authority
- Discovery tool configuration: scope, schedule, credentials handling and OT exclusions
- Network diagram showing segments, DHCP sources and passive sensor locations
- Half-yearly reconciliation and attestation records

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 7-2. Assessment testing procedures, Control 1

Test ID	Method	Testing procedure	Result
TP-C01-01	**EXAMINE**	1.1: Examine the asset management policy and register. Confirm the scope covers end-user, mobile, network, server, IoT, virtual, cloud and regularly connecting non-enterprise devices, and that each record holds hostname, hardware address, static IP where used, owner, department and approval status.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C01-02	**SAMPLE**	1.1: Select a sample of 15–25 devices observed physically on site, in the EDR or MDM console and in a cloud console, and trace each to the register; then select a sample from the register and trace it back to a live device or a disposal record. Record completeness and accuracy rates.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C01-03	**INSPECT**	1.1: Inspect evidence of the last two register reviews and confirm that they took place no more than six months apart and resulted in documented corrections.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C01-04	**SAMPLE**	1.2: For a period of at least eight weeks, inspect the weekly unauthorised-device review records. Confirm a review happened each week and sample unknown-device tickets to verify each was approved, isolated, denied remote access or removed, with dates.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C01-05	**RE-PERFORM**	1.2: With management's agreement, connect a test device not in the register to a user network segment and observe whether it is detected and handled within the documented timeframe.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C01-06	**INSPECT**	1.3: Inspect the active discovery tool's schedule and scope. Compare the scanned ranges with the network diagram and IPAM to identify omitted subnets, and review run logs for a sample month to confirm daily execution.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C01-07	**EXAMINE**	1.4: Obtain the list of all DHCP-serving devices (servers, firewalls, wireless controllers, branch routers) and confirm logging is enabled and forwarded centrally for each. Examine a sample of weekly reconciliations of DHCP leases against the register.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C01-08	**RE-PERFORM**	1.4: Take one week of DHCP logs, extract unique MAC addresses and compare them independently with the register; investigate any unexplained differences with IT.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C01-09	**OBSERVE**	1.5: Observe the passive discovery console, confirm sensor locations match the documented design, and inspect a sample of weekly reviews showing passive findings compared with the register and resulting updates.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C01-10	**INTERVIEW**	1.1–1.5: Interview the register owner and a sample of department heads to confirm they understand their responsibilities and how devices are added, transferred and retired.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Sample in both directions: from the real estate to the register (completeness) and from the register to the estate (accuracy and stale records). Use the EDR, MDM, directory and cloud consoles, plus a physical walk of at least one office and one branch or plant, as independent populations. For a population under 250 devices, 15–25 items is usually sufficient; for larger estates use 25–40 items stratified by asset class and location, and always include IoT, network devices and cloud instances. For weekly and daily routines, test a period of at least two months and select a minimum of four to eight occurrences, including at least one holiday or month-end week.

P Interview Questions

Interviewee	Question
IT / infrastructure manager	How does a new laptop, server or cloud instance get into the register, and what stops one from being missed?
IT / infrastructure manager	Walk me through the last unknown device you found. How was it found, who decided what to do, and how long did it take?
OT / plant engineering lead	How are plant devices identified and recorded, and what discovery methods are allowed on the plant network?
Department head	When did you last confirm the list of devices assigned to your team, and what changed?
MSP account manager	What inventory and unknown-device reporting does your contract require, and how often do you deliver it?

Q Technical and Process Verification

- The register exists, is owned and contains the required identifying fields for every asset class in scope.
- Two-way sampling shows high completeness and accuracy, with stale records explained.
- Unknown devices are reviewed at least weekly with documented outcomes.

- Discovery scans (IG2) run daily across all ranges, and DHCP logs are used weekly.
- Passive discovery (IG3) covers the segments where it matters most and findings are acted on.
- The register is used as the denominator for other coverage metrics.

R Expected Evidence

- Asset management policy and register export
- Two-way sample worksheet with completeness and accuracy results
- Half-yearly review records and attestations
- Weekly unknown-device review log and sample tickets
- Quarantine VLAN or NAC configuration screenshots
- Active discovery scope and run history
- DHCP logging configuration and weekly reconciliation output
- Passive sensor placement diagram and weekly review records

S Evaluation Criteria

Implemented

- The register is complete, accurate and reviewed at least half-yearly, and samples trace both ways with few exceptions.
- Unknown devices are reviewed weekly and resolved with evidence.
- For the target IG, discovery automation runs at the required frequency and feeds the register.

Partially implemented

- A register exists but omits asset classes such as IoT, cloud or personal devices, or lacks owners.
- Unknown-device reviews happen but irregularly or without recorded outcomes.
- Discovery tools run but do not cover all ranges or are not reconciled with the register.

Not implemented

- No maintained register, or one that has not been updated in over a year.
- No routine to find or handle unknown devices.
- Required discovery tools for the target IG are absent.

T Common Gaps and Findings

- Condition: the register excludes CCTV recorders, biometric readers and printers. Criteria: 1.1 requires all devices that can store or process data. Effect: unpatched IoT devices with default credentials sit on the LAN unmonitored.
- Condition: unknown devices are noted in scan reports but no action is recorded. Criteria: 1.2 requires weekly resolution. Effect: rogue or personal devices remain connected indefinitely.
- Condition: active scans cover head office only, not the 12 branch networks. Criteria: 1.3 requires all enterprise networks. Effect: branch devices, often the least managed, are invisible.
- Condition: DHCP is served by branch firewalls with logging disabled. Criteria: 1.4 expects logging on all DHCP sources. Effect: new devices at branches cannot be detected or traced after an incident.
- Condition: cloud instances are not recorded because they are 'managed by DevOps'. Criteria: 1.1 includes cloud assets. Effect: internet-exposed instances escape patching and logging.

U Remediation Guidance

- Extend the register schema and run a one-off discovery sprint for IoT, network and cloud assets, assigning owners for each.
- Introduce a weekly unknown-device review with a ticket per device and a defined isolation option, and report the backlog monthly.
- Extend discovery scope to every subnet listed in IPAM, using a lightweight scanner or agent at branches.
- Enable DHCP logging on all branch firewalls and forward logs to the central SIEM.
- Pull cloud inventories by API daily into the CMDB and tag every instance with an owner and environment.
- Make register updates a mandatory step in procurement, joiner-leaver and disposal workflows.

V Monitoring Metrics

- Register completeness: percentage of devices seen by discovery, EDR or MDM that are in the register (target 98% or more).
- Register accuracy: percentage of register records traced to a live device or disposal record (target 95% or more).
- Mean time to resolve an unknown device, in days (target 7 or fewer).

- Percentage of network ranges covered by daily active discovery (IG2).
- Number of unknown devices detected per month, trended.

W Related Controls and Maturity Indicators

- Control 2 (software runs on the assets inventoried here)
- 4.1 and 4.2 (secure configuration applies to every inventoried asset)
- 7.1 (vulnerability management depends on the asset list)
- 10.1 (anti-malware coverage measured against the register)
- 12.1 and 13.5 (network infrastructure and remote device access)
- 11.1 (recovery planning needs the asset list)
- 15.1 (service provider assets)

Initial	Defined	Managed	Optimised
Devices are known informally or through scattered lists; unknown devices are discovered by accident.	A policy and single register with mandatory fields exist, with a documented weekly unknown-device routine.	Discovery is automated (active scans, DHCP and cloud feeds), reconciliation is routine and coverage metrics are reported monthly.	Active, passive and agent sources are correlated in near real time, NAC enforces approval at connection, and the register drives all other coverage measures.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A 300-employee Coimbatore textile exporter, with a head office, two spinning units and a design studio in Tiruppur, kept its asset list in the finance team's fixed-asset ledger. It recorded purchase cost and depreciation but not hostnames, MAC addresses or owners, and it had no entries for the 60 CCTV cameras, three network recorders or the biometric attendance terminals at each unit.

After a ransomware infection that started on an unmanaged Windows 7 PC used to run a dyeing machine, the company adopted Control 1 at IG1 with an eye on IG2. The IT manager exported computers from the directory, devices from the MDM and clients from each unit's Wi-Fi controller, merged them in a spreadsheet and walked each site with a checklist. The exercise found 41 devices no one had recorded, including two personal NAS boxes and a contractor's laptop that had been connected for eight months.

The firm set a rule that the register is updated before any device is issued and when any device is scrapped, and introduced a Monday review of new Wi-Fi and switch clients. Unknown devices are moved to a guest VLAN until claimed. Six months later the exporter added a weekly open-source network scan across all three sites and began comparing DHCP leases from the branch firewalls. By the next half-yearly review, completeness stood at 97%, and the plant engineer had added the dyeing-machine controllers with a note that they must only be scanned passively.

WP-C01: use the workpaper format shown in Appendix H.

CHAPTER 8 · CIS CONTROL 2

Inventory and Control of Software Assets

CIS CONTROL 2 · 7 SAFEGUARDS · 3 IN IG1

Inventory and Control of Software Assets

CIS Controls v8.1 · titles quoted verbatim | WP-C02

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 2 — Inventory and Control of Software Assets

Control 2 is the software counterpart of Control 1. Once the enterprise knows which devices it has, it needs to know what runs on them, whether each piece of software is approved and still supported, and whether anything else can run at all. The Control moves from knowledge to enforcement. IG1 Safeguards build an authorised software list, keep unsupported software out of it and remove what should not be there. IG2 automates discovery and introduces allowlisting of applications and code libraries. IG3 brings scripts under the same discipline. Done well, this Control shrinks the attack surface, gives vulnerability management a reliable product list and makes many malware techniques fail outright, because the malicious executable or script is simply not permitted to start.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 8-1. Safeguards of CIS Control 2, Inventory and Control of Software Assets

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
2.1	**“Establish and Maintain a Software Inventory”**	Software	Identify	IG1	Maintain a register of the software the enterprise has licensed and installed across its assets, recording at least the product, publisher, when it was first installed or used and why the business needs it, plus version, source, deployment method, licence count and retirement date where useful. Review it at least every six months.
2.2	**“Ensure Authorized Software is Currently Supported”**	Software	Identify	IG1	Only software that its publisher still supports (with security fixes) may be marked as authorised. Where the business genuinely cannot retire an unsupported product, a documented exception records compensating controls and a named risk acceptance; anything else unsupported is treated as unauthorised. Check support status at least monthly.
2.3	**“Address Unauthorized Software”**	Software	Respond	IG1	Find software running on enterprise assets that is not authorised and either uninstall it or put it through a documented exception. Do this at least monthly.
2.4	**“Utilize Automated Software Inventory Tools”**	Software	Detect	IG2	Use software inventory tooling wherever practical so that installed software is discovered and recorded automatically rather than by survey.
2.5	**“Allowlist Authorized Software”**	Software	Protect	IG2	Apply a technical control, typically application allowlisting, so that only authorised software can run or be reached on enterprise assets, and reassess the rules at least every six months.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
2.6	**“Allowlist Authorized Libraries”**	Software	Protect	IG2	Extend allowlisting to the code modules that programs load, such as Windows DLL and OCX files and Linux shared objects, so that unapproved libraries cannot be injected into running processes. Reassess at least every six months.
2.7	**“Allowlist Authorized Scripts”**	Software	Protect	IG3	Control which scripts may run, such as PowerShell and Python files, by using signing, version control and execution policy, and block the rest. Reassess at least every six months.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
2.1	**1.** Agree the record format: title, publisher, first install or use date, business purpose and business owner as mandatory; version, source URL or app store, deployment method, licence count and decommission date as optional but encouraged. **2.** Include SaaS subscriptions, browser extensions, mobile apps, server software, database engines, firmware-managed appliances and in-house applications, not only desktop packages. **3.** Seed the register from licence records, purchase orders, endpoint management reports and SaaS expense data, and assign an owner per entry. **4.** Review half-yearly and on major change, removing retired items and capturing new ones.	• Software register export with mandatory fields • Last two review records • Owner assignments for business-critical software
2.2	**1.** Add support-status and end-of-support date fields to the register, sourced from publisher life-cycle pages. **2.** Run a monthly review that flags products reaching end of support in the next 6–12 months, so replacement is planned before the date. **3.** Create an exception template covering business reason, compensating controls (isolation, restricted access, extra monitoring), residual risk, approver and expiry date. **4.** Reclassify unsupported software without a current exception as unauthorised and route it to 2.3.	• Register showing support status and dates • Monthly support-review records • Approved exception forms with compensating controls and expiry
2.3	**1.** Compare discovered software (from 2.4 tooling or manual review) with the authorised list each month. **2.** Define the response: notify the user and owner, remove remotely or via a service desk ticket, or raise an exception. **3.** Track each case to closure and escalate repeat offenders through HR or line management.	• Monthly unauthorised-software reports • Removal tickets or exception records • Trend of unauthorised installs over time
2.4	**1.** Use the software inventory features of endpoint management, MDM or EDR agents, and of server configuration tools, to collect installed packages across Windows, macOS, Linux and mobile. **2.** Extend discovery to cloud workloads and container images, and to SaaS use through identity-provider or CASB reports. **3.** Normalise product names and versions and feed them into the register for comparison with the authorised list.	• Tool configuration showing agent coverage • Automated inventory report • Coverage figure compared with the asset register

Safeguard	Practical steps	Evidence
2.5	1. Start in audit mode on a pilot group to learn what actually runs, then build rules based on publisher signatures, file paths controlled by administrators and hashes. 2. Enforce on high-risk systems first (servers, admin workstations, kiosks, finance PCs), then on general endpoints. 3. Set a fast, documented process for requesting new software so that users do not bypass controls. 4. Review the rule set half-yearly to remove stale rules and confirm no wide-open exceptions.	• Allowlisting policy and rule set • Enforcement-mode status per device group • Block event logs and half-yearly rule review record
2.6	1. Enable library (DLL / shared-object) rule enforcement in the allowlisting tool after testing for performance and compatibility. 2. Restrict write access to library directories and use signed-library policies where the platform supports them. 3. Monitor and review blocked library loads, which often reveal DLL side-loading attempts.	• Library-rule configuration • Logs of blocked library loads • Half-yearly review record
2.7	1. Keep administrative and automation scripts in a version-controlled repository with peer review. 2. Sign approved scripts and set interpreters to run only signed or allowlisted scripts (for example, PowerShell constrained language mode with signed scripts). 3. Block or alert on script execution from user-writable locations such as Downloads and temp folders, and log script activity centrally.	• Script-control policy and interpreter configuration • Repository and signing records for approved scripts • Logs of blocked scripts

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
An IG1 enterprise must keep a software register with an owner and business purpose per item (2.1), allow only supported software onto the authorised list with documented exceptions for anything unavoidable (2.2), and remove or formally except unauthorised software at least monthly (2.3). A small firm can do this by removing local admin rights, keeping a one-page approved list and checking the endpoint tool's installed-software report once a month.	IG2 adds automated software inventory across all assets (2.4), technical allowlisting so that only authorised software executes (2.5), and extension of allowlisting to libraries loaded into processes (2.6). These require tooling and testing, and usually a staged roll-out.	IG3 adds control over scripts (2.7): only signed or otherwise approved scripts may run, and everything else is blocked. This targets fileless and living-off-the-land techniques used against mature, high-value targets.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 2.1 → 5.9 Inventory of information and other associated assets; 5.32 Intellectual property rights (licences)
- 2.2 → 8.8 Management of technical vulnerabilities; 5.9
- 2.3 → 8.19 Installation of software on operational systems; 5.10 Acceptable use of information and other associated assets
- 2.4 → 5.9; 8.9 Configuration management
- 2.5 → 8.19; 8.7 Protection against malware
- 2.6 → 8.7; 8.19
- 2.7 → 8.19; 8.7; 8.32 Change management; 8.4 Access to source code

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: ID.AM-02 (software inventories), PR.PS-02 (software maintained, replaced and removed), PR.PS-05 (unauthorised software prevented), DE.CM-09 (computing software monitored) (Srida IT mapping)

- NIST SP 800-53 Rev. 5: CM-7 Least Functionality including CM-7(5) authorised software allow-by-exception; CM-8; CM-10 Software Usage Restrictions; CM-11 User-installed Software; SA-22 Unsupported System Components
- PCI DSS v4.0.1: Requirement 6.3.2 (inventory of bespoke and custom software and third-party components) and 12.5.1

F India Regulatory Touchpoints

- SEBI CSCRF (2024): expectations on software asset inventory, patching and decommissioning of unsupported systems for regulated entities
- RBI IT governance and cyber security directions for banks and NBFCs: application inventory, version control and restrictions on unauthorised software
- IRDAI Information and Cyber Security Guidelines (2023): asset and software management, and end-of-life handling for insurers
- DPDP Act 2023 s.8(5): running unsupported software that exposes personal data may undercut the claim of reasonable security safeguards

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Most intrusions need code to run on an enterprise device: a malicious attachment, a fake installer, a remote-access tool, a credential dumper or a ransomware binary. Where users can install and run anything, attackers have the same freedom. Unmanaged software also carries vulnerabilities nobody tracks: an old PDF reader, a pirated design suite, a browser extension with excessive permissions, a remote-support tool left over from a vendor visit. Attackers increasingly use legitimate tools and scripts (living off the land), so control over scripts and libraries matters as much as control over installers.

Unsupported software is a specific danger because security fixes stop entirely. Organisations still running end-of-life operating systems on factory PCs, outdated database versions behind business applications or old Java runtimes for legacy tools accept vulnerabilities that will never be fixed. Software sprawl also increases exposure in publisher licence audits, which a reliable register makes far easier to answer.

Indian regulators expect this discipline. SEBI's CSCRF, RBI's IT governance directions and IRDAI's guidelines refer to approved software, patching and removal of end-of-life systems. Under the DPDP Act a personal data breach caused by a known-vulnerable, unsupported application would be hard to defend as a reasonable security safeguard. For SMEs, a short authorised list and blocking of user installs is one of the cheapest, highest-return controls available.

I Applicability

Applies to every enterprise. A 40-person firm meets IG1 by removing local administrator rights, keeping a short approved list in a shared document and checking the endpoint tool's report monthly. Cloud- and SaaS-heavy organisations must count SaaS subscriptions, OAuth-connected apps, browser extensions and container images as software; identity-provider and expense data are good discovery sources. OT environments often depend on unsupported operating systems tied to machine vendors; these need recorded exceptions with strong isolation rather than pretending they are compliant. Allowlisting on OT engineering workstations is frequently easier than on office PCs because the software set is stable. Where an MSP manages endpoints, the contract should cover inventory reporting, end-of-support alerts and allowlisting management.

J Implementation Guidance

1. Assign a software asset owner (often IT operations) and agree what counts as software: installed packages, SaaS, extensions, mobile apps, server components and in-house code.
2. Build the initial register from licences, purchase records and the endpoint tool's installed-software report, and give each entry a business owner and purpose.
3. Add support status and end-of-support dates, and agree the exception process for unavoidable unsupported products.
4. Remove local administrator rights from standard users and publish a self-service catalogue of approved software.
5. Start a monthly cycle: compare installed software with the authorised list, remove or except outliers and check support status.
6. At IG2, extend automated inventory to all platforms and cloud workloads, then pilot allowlisting in audit mode, tune and enforce in stages.
7. Enable library rules after allowlisting is stable, and monitor blocked loads.

8. At IG3, move administrative scripts into version control, sign them and enforce script execution policies.
9. Review the register and allowlisting rules at least half-yearly, and report metrics to management.

K Tools and Automation

- Endpoint management / MDM with software inventory: lists installed applications across devices and supports remote removal.
- Application allowlisting (application control) built into operating systems or EDR platforms: enforces publisher, path and hash rules.
- EDR: detects unauthorised and malicious execution and records process and script activity.
- Software asset management (SAM) or CMDB: normalises software titles, tracks licences and support dates.
- Open-source osquery or Wazuh agents: query installed packages and running processes across servers and endpoints.
- Software composition analysis and container image scanners: identify libraries and components in in-house applications and images.
- Identity provider / CASB reports: reveal SaaS applications and OAuth grants in use.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
IT operations / endpoint team	Maintains the register, runs inventory tools, removes unauthorised software and manages allowlisting rules.
Business software owners	Justify each product, confirm business need and fund replacement before end of support.
CISO / information security	Sets policy, approves exceptions for unsupported software and reviews allowlisting coverage.
Procurement / finance	Route software purchases and subscriptions through IT so they are registered.
Development / DevOps lead	Controls libraries and scripts in in-house code and pipelines, and maintains signing.
Service desk	Handles software requests and user communication when software is blocked or removed.

M Documentation and Records

- Software management policy covering authorisation, installation rights and support status
- Software register with owners, purpose and support dates
- Exception register for unsupported or unauthorised software with compensating controls and expiry
- Monthly unauthorised-software and support-status review records
- Allowlisting standard, rule sets and change records
- Script management standard and code-signing procedures

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 8-2. Assessment testing procedures, Control 2

Test ID	Method	Testing procedure	Result
TP-C02-01	**EXAMINE**	2.1: Examine the software register and confirm each entry records title, publisher, first install or use date and business purpose, and that SaaS, server and in-house software are included. Confirm half-yearly reviews took place.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C02-02	**SAMPLE**	2.1: Select a sample of 10 endpoints and 5 servers, extract installed software and trace each product to the register; separately sample 10 register entries and confirm they are still in use or marked retired.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C02-03	**INSPECT**	2.2: Inspect the register for support status. For a sample of 15 authorised products, check the publisher's life-cycle information to confirm they remain supported; inspect monthly review records for the last three months.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C02-04	**EXAMINE**	2.2: Examine all exceptions for unsupported software and confirm each has a business reason, compensating controls, residual-risk acceptance by an authorised person and an expiry date; verify compensating controls on one sampled system.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C02-05	**SAMPLE**	2.3: Select three monthly unauthorised-software reports from the last six months and, for a sample of flagged items, confirm removal or an approved exception, with dates.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C02-06	**INSPECT**	2.4: Inspect the automated inventory tool's coverage report and compare the number of reporting assets with the asset register from Control 1; investigate devices with no software data.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C02-07	**RE-PERFORM**	2.5: On a sample of enforced devices, attempt to run a harmless, unapproved executable from a user-writable folder and confirm it is blocked and the event logged.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C02-08	**EXAMINE**	2.5: Examine the allowlisting rule set for broad rules (for example, allowing all files in user-writable paths) and confirm the rule set was reassessed within the last six months.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C02-09	**INSPECT**	2.6: Inspect allowlisting configuration to confirm library rules are enforced on in-scope systems, and inspect logs for blocked library loads and follow-up of suspicious ones.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C02-10	**RE-PERFORM**	2.7: On a sample system, attempt to run an unsigned PowerShell or Python test script from a user folder and confirm it is blocked; confirm approved scripts are signed and held in version control.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C02-11	**INTERVIEW**	2.1–2.7: Interview the endpoint team and a business software owner about how new software is requested, approved, registered and retired, and how end-of-support dates are tracked.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Use the asset register from Control 1 as the population of devices, and stratify the sample across operating systems, business units and device roles (servers, admin workstations, general users, OT). For software lists, sample both from installed software to the register (completeness) and from the register to installed software (accuracy). For monthly routines, test at least three months; for half-yearly reviews, test the last two. Re-performance of allowlisting should cover at least one device from each enforcement group.

P Interview Questions

Interviewee	Question
IT operations manager	How do you find out that someone has installed software that is not on the approved list, and what happens next?
IT operations manager	Which products in use will reach end of support in the next 12 months, and what is the plan for each?
Business software owner	Why does the business still need this unsupported application, and what controls protect it?
Endpoint engineer	How were the allowlisting rules built, how often are they reviewed and who can change them?
DevOps lead	How are scripts used in automation approved, stored and signed?

Q Technical and Process Verification

- A software register exists with owners, purpose and support status.
- Unsupported software is either retired or covered by a current, approved exception.
- Unauthorised software is detected and handled at least monthly.

- Automated inventory covers nearly all assets in the Control 1 register (IG2).
- Allowlisting blocks unapproved executables and libraries on in-scope systems (IG2).
- Only approved scripts can run on in-scope systems (IG3).

R Expected Evidence

- Software policy and register export
- Support-status review records and end-of-support forecast
- Exception register with approvals
- Monthly unauthorised-software reports and removal tickets
- Inventory tool coverage report
- Allowlisting rules, enforcement status and block logs
- Script signing and execution-policy configuration
- Re-performance screenshots of blocked execution

S Evaluation Criteria

Implemented

- The register is complete and current, with support status checked monthly and exceptions documented.
- Unauthorised software is removed or excepted every month with evidence.
- For the target IG, allowlisting (and script control at IG3) is enforced and reviewed half-yearly.

Partially implemented

- A register exists but omits SaaS or server software, or lacks business purpose and owners.
- Unsupported software is known but exceptions lack compensating controls or expiry.
- Allowlisting runs in audit mode only, or covers a small subset of systems.

Not implemented

- No software register or authorised list.
- Users install software freely and no review takes place.
- No technical execution control at the target IG.

T Common Gaps and Findings

- Condition: 30% of office PCs run an end-of-life PDF reader. Criteria: 2.2 allows only supported software without exception. Effect: known exploitable vulnerabilities remain on user devices.
- Condition: all staff have local admin rights. Criteria: 2.3 requires control of unauthorised software. Effect: pirated and potentially trojanised software spreads freely.
- Condition: the software register excludes SaaS and browser extensions. Criteria: 2.1 covers all licensed software. Effect: data flows to unvetted services and permissions go unreviewed.
- Condition: allowlisting has been in audit mode for two years. Criteria: 2.5 requires technical enforcement. Effect: the control provides visibility only, not prevention.
- Condition: legacy machine-control PCs run an unsupported operating system without an exception. Criteria: 2.2 requires documented risk acceptance and mitigations. Effect: unmanaged risk on production-critical systems.

U Remediation Guidance

- Remove local admin rights and introduce a self-service approved catalogue.
- Add end-of-support fields and a 12-month forecast to the register, with budgeted replacement.
- Record exceptions for unavoidable unsupported systems with network isolation and extra monitoring.
- Extend discovery to SaaS via identity-provider reports and browser extension policies.
- Move allowlisting from audit to enforcement in waves, starting with servers and finance PCs.
- Version-control and sign administrative scripts before enforcing script policies.

V Monitoring Metrics

- Percentage of assets reporting software inventory (target 98% or more).
- Number of unsupported products without an approved exception (target zero).
- Number of unauthorised installations detected per month, and median days to remove.
- Percentage of devices with allowlisting in enforcement mode (IG2).
- Percentage of production scripts that are signed and in version control (IG3).

W Related Controls and Maturity Indicators

- Control 1 (asset inventory is the denominator)
- 4.1 (secure configuration includes software baselines)
- 5.4 (restricting admin privileges supports 2.3)
- 7.3 and 7.4 (patch management needs the product list)
- 9.4 (browser and email extensions)
- 10.1 (anti-malware complements allowlisting)
- 16.4 (third-party components in in-house software)

Initial	Defined	Managed	Optimised
Software is installed ad hoc; there is no authorised list and no visibility of support status.	A policy, register and authorised list exist, with monthly reviews and documented exceptions.	Inventory is automated, end-of-support is forecast and allowlisting is enforced on most systems.	Allowlisting covers applications, libraries and scripts; software requests are self-service and measured; exceptions are rare and time-bound.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A 600-employee Pune NBFC with 45 branches let branch staff install tools to help with collections and customer contact. A routine RBI inspection preparation review found 212 distinct software titles across branch PCs, including three remote-access tools, unlicensed office suites and an end-of-life operating system on loan-processing PCs.

The NBFC adopted Control 2 starting at IG1. It removed local administrator rights, published an approved catalogue of 38 products and used its endpoint management tool's inventory to produce a monthly report of anything else. Each branch manager was named as owner for branch-specific tools. The IT team added end-of-support dates and found that the loan-processing application needed an operating system version that would lose support within eight months; the business funded an upgrade and, in the meantime, an exception was approved by the CISO with network isolation and enhanced logging.

In the second year the NBFC moved toward IG2. It ran application control in audit mode for six weeks, built publisher-based rules and enforced them on head-office finance PCs, then on branches in waves. Library rules followed after testing with the core lending application. Unauthorised installs fell from around 90 per month to under five, and the next inspection noted a reliable software inventory. The company has not adopted 2.7 yet, but its DevOps team now keeps automation scripts in a version-controlled repository as a first step.

WP-C02: use the workpaper format shown in Appendix H.

CHAPTER 9 · CIS CONTROL 3

Data Protection

CIS CONTROL 3 · 14 SAFEGUARDS · 6 IN IG1

Data Protection

CIS Controls v8.1 · titles quoted verbatim | WP-C03

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 3 — Data Protection

Control 3 is about the data itself rather than the devices or software around it. It asks the enterprise to decide what data it has, how sensitive each kind is, who is responsible for it, where it lives and travels, who may touch it, how long it is kept and how it is destroyed, and then to protect it with encryption, segmentation, data loss prevention and logging in proportion to that sensitivity. With 14 Safeguards it is one of the largest Controls, and it is where security and privacy meet. The IG1 Safeguards establish governance and the basics: a data management process, an inventory of sensitive data, need-to-know permissions, retention and disposal rules, and encryption on end-user devices. IG2 adds classification, data flow documentation, encryption in transit, at rest and on removable media, and segmentation by sensitivity. IG3 adds automated data loss prevention and logging of access to sensitive data. For Indian enterprises Control 3 is the most direct technical bridge to the Digital Personal Data Protection Act 2023 and its Rules.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 9-1. Safeguards of CIS Control 3, Data Protection

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
3.1	**“Establish and Maintain a Data Management Process”**	Data	Govern	IG1	Write down and run a process that governs enterprise data from creation to destruction: how sensitive each kind of data is, who owns it, how it must be handled, how long it may be kept and how it must be destroyed. Review the process at least yearly and whenever a significant change (a new regulation, acquisition, major system or business line) affects it.
3.2	**“Establish and Maintain a Data Inventory”**	Data	Identify	IG1	Build and keep a register of the enterprise's data, driven by the data management process, that at minimum identifies where sensitive data (including personal data) lives, in which systems, under whose ownership and for what purpose. Update it at least yearly, starting with the most sensitive sets.
3.3	**“Configure Data Access Control Lists”**	Data	Protect	IG1	Restrict access to data according to each user's need to know, by setting permissions on local and network file systems, databases, cloud storage and applications, so that nobody can read or change data their role does not require.
3.4	**“Enforce Data Retention”**	Data	Protect	IG1	Keep each category of data for no less than the period law, regulation or business need requires and no longer than the documented maximum, and make the rules operate in systems rather than only on paper.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
3.5	**“Securely Dispose of Data”**	Data	Protect	IG1	Destroy data at the end of its retention period, or on a valid erasure request, by a method suited to its sensitivity and the medium it sits on, and keep a record that disposal happened.
3.6	**“Encrypt Data on End-User Devices”**	Data	Protect	IG1	Turn on full-disk or equivalent encryption on laptops, desktops, tablets and phones that hold sensitive data, so a lost or stolen device does not expose it.
3.7	**“Establish and Maintain a Data Classification Scheme”**	Data	Identify	IG2	Define one classification scheme for the whole enterprise, with a small number of clear levels and criteria for assigning them, and use it to drive handling rules. Review it at least yearly or when significant change occurs.
3.8	**“Document Data Flows”**	Data	Identify	IG2	Document how sensitive data moves into, through and out of the enterprise, including to and from service providers, aligned with the data management process. Review at least yearly or on significant change.
3.9	**“Encrypt Data on Removable Media”**	Data	Protect	IG2	Encrypt any data written to USB drives, external disks, memory cards or other removable media, or block such media where it is not needed.
3.10	**“Encrypt Sensitive Data in Transit”**	Data	Protect	IG2	Protect sensitive data travelling across any network, internal or external, with strong encryption such as current TLS versions and SSH.
3.11	**“Encrypt Sensitive Data at Rest”**	Data	Protect	IG2	Encrypt sensitive data stored on servers, databases, applications and cloud storage. Storage-level (server-side) encryption is the floor; application-level or client-side encryption, where storage administrators cannot see plain text, gives stronger protection.
3.12	**“Segment Data Processing and Storage Based on Sensitivity”**	Data	Protect	IG2	Separate the systems and storage that handle sensitive data from those meant for less sensitive data, and do not process high-sensitivity data on platforms intended for lower-sensitivity use.
3.13	**“Deploy a Data Loss Prevention Solution”**	Data	Protect	IG3	Use automated data loss prevention tooling (host-based, network, email, cloud or a combination) to find sensitive data wherever it is stored, processed or sent, including at service providers, and feed the results into the data inventory.
3.14	**“Log Sensitive Data Access”**	Data	Detect	IG3	Record who accesses sensitive data, including when it is changed or deleted, so misuse can be detected and investigated.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
3.1	1. Draft a data management standard that links to the classification scheme (3.7), names data owners by business function and sets handling rules per class for storage, sharing, transfer, printing and disposal. 2. Embed legal and regulatory retention drivers: DPDP Act purpose limitation and erasure, sector record-keeping rules (RBI, SEBI, IRDAI, PMLA, tax and company law) and contractual obligations. 3. Assign a process owner (often the DPO, privacy lead or CISO) and define how data owners approve exceptions. 4. Schedule an annual review, and add triggers for out-of-cycle review such as the commencement of DPDP Rules obligations or a new processor relationship.	• Approved data management standard with version history • Named data owners per data domain • Review records for the last cycle, including any triggered by significant change
3.2	1. Define inventory fields: data set, category and classification, personal-data indicator, data principals affected (customers, employees, patients, children), purpose, system or repository, location (including cloud region and processor), owner, retention rule and volume estimate. 2. Collect entries through owner workshops and questionnaires, then validate with discovery tooling or database schema reviews. 3. Link the inventory with the asset register (Control 1) and software register (Control 2) so every sensitive data set maps to the systems that hold it. 4. Reuse the inventory as the backbone of the record of processing used for DPDP accountability, and update it at least annually and on any new processing.	• Data inventory or record of processing • Evidence of annual update and owner sign-off • Mapping of sensitive data sets to systems
3.3	1. Define role-based access groups per data set, approved by the data owner, rather than granting access to individuals. 2. Remove broad grants such as 'Everyone', 'Domain Users', public links and anonymous cloud buckets from repositories holding sensitive data. 3. Apply database-level and application-level permissions, including row or field restrictions for highly sensitive fields such as Aadhaar numbers, bank details or diagnoses. 4. Re-certify access to sensitive repositories periodically with data owners, linking to Controls 5 and 6.	• Permission reports for sampled repositories • Access group definitions approved by data owners • Access review records
3.4	1. Build a retention schedule listing, per data category, the minimum period (statutory or contractual) and the maximum period (purpose served, consent withdrawn, or a fixed outer limit), and the event that starts the clock. 2. Resolve conflicts explicitly, for example between DPDP erasure once the purpose is served and sector rules requiring KYC or transaction records to be held for years. 3. Configure retention in systems: mailbox and file retention policies, database archival jobs, backup expiry and log rotation consistent with CERT-In and DPDP Rules log retention expectations. 4. Run a periodic retention sweep that identifies data past its maximum and routes it to secure disposal (3.5).	• Retention schedule with minimum and maximum periods • System retention configurations • Retention sweep reports

Safeguard	Practical steps	Evidence
3.5	1. Define disposal methods per class and medium: secure deletion or cryptographic erasure for disks and cloud volumes, degaussing or shredding for media, cross-cut shredding for paper, and vendor deletion certificates for SaaS and processors. 2. Use approved e-waste recyclers registered under the E-Waste (Management) Rules for hardware, with certificates of destruction tied to asset tags. 3. Include backups and copies in the disposal plan, or document the backup expiry that achieves deletion in due course. 4. Log each disposal event with data set, method, date and approver, and confirm processors delete data at contract end.	• Disposal procedure by class and medium • Certificates of destruction linked to asset tags • Disposal log and processor deletion confirmations
3.6	1. Enable native full-disk encryption (BitLocker on Windows, FileVault on macOS, LUKS / dm-crypt on Linux, built-in encryption with a device passcode on mobile). 2. Escrow recovery keys centrally in the directory or MDM, with restricted access and logging. 3. Enforce encryption through MDM or group policy, and report non-compliant devices for remediation. 4. Cover the devices of contractors and BYOD users that hold sensitive data, through MDM enrolment or managed containers.	• MDM or endpoint encryption compliance report • Recovery key escrow configuration • Policy requiring encryption
3.7	1. Choose three to five levels (for example, Public, Internal, Confidential, Restricted) with plain-language criteria and examples drawn from the business. 2. Add regulatory tags that cut across levels: personal data, children's data, Aadhaar, financial account or card data, health data, KYC and data under sector localisation rules. 3. Map each level and tag to handling rules from 3.1 (encryption, sharing, retention, disposal), and train staff with short examples. 4. Apply labels where practical: document templates, email labels, database metadata and storage tags.	• Approved classification scheme and handling matrix • Examples of labelled documents or repositories • Review record
3.8	1. Draw data flow diagrams for key processes (customer onboarding, payroll, patient care, payments) showing sources, systems, storage, processors and destinations, including cross-border transfers. 2. Record for each flow the data categories, classification, transfer method and protection (encryption, tokenisation). 3. Identify flows to processors and other fiduciaries, and confirm contracts and DPDP cross-border restrictions are considered. 4. Update diagrams when systems, vendors or processes change, and at least annually.	• Data flow diagrams with dates and owners • List of processor and third-party flows • Review record
3.9	1. Decide where removable media is allowed at all; block it by default through endpoint or MDM policy and permit by exception. 2. Where allowed, enforce encryption on write (for example, BitLocker To Go or hardware-encrypted drives) and issue enterprise-owned media only. 3. Log removable media use and review exceptions periodically.	• Removable media policy and endpoint configuration • List of approved encrypted media • Usage logs and exception records

Safeguard	Practical steps	Evidence
3.10	**1.** Enforce TLS 1.2 or higher (preferably 1.3) on websites, APIs, email gateways and internal applications that carry sensitive data, disabling weak ciphers and older protocols. **2.** Replace clear-text protocols (FTP, Telnet, HTTP, unencrypted database connections) with SFTP, SSH, HTTPS and encrypted database links. **3.** Manage certificates centrally with expiry monitoring, and use encrypted channels for file exchange with banks, processors and regulators. **4.** Scan regularly for weak protocols and expired certificates.	• TLS configuration scan results • Inventory of certificates with expiry • Evidence that clear-text protocols are disabled
3.11	**1.** Enable encryption at rest for databases (transparent data encryption), file servers, storage arrays, cloud volumes, object storage and backups. **2.** For the most sensitive fields (Aadhaar numbers, card numbers, health records), add field- or application-level encryption, tokenisation or vaulting. **3.** Manage keys in a key management system or HSM, separate key custodians from data administrators and rotate keys on a schedule. **4.** Verify encryption state through configuration reports and cloud posture tools.	• Encryption-at-rest configuration reports • Key management procedure and key inventory • Evidence of field-level protection for highest-risk data
3.12	**1.** Group systems into zones by the highest classification of data they process, using network segmentation, separate cloud accounts or projects, and separate databases. **2.** Prevent sensitive data from entering test, development and analytics environments unless masked or synthetic. **3.** Restrict traffic between zones to defined flows from 3.8, enforced by firewalls or security groups.	• Zone design linked to classification • Firewall or security group rules between zones • Evidence of masked data in non-production
3.13	**1.** Define detection policies for India-specific identifiers (Aadhaar, PAN, bank account and IFSC, card numbers, health identifiers) and enterprise-specific data, with validation to reduce false positives. **2.** Start with discovery and monitoring on endpoints, file shares, email and cloud storage, then add blocking for the highest-risk channels. **3.** Feed discovery results into the data inventory (3.2) and review incidents with data owners. **4.** Extend coverage to sanctioned SaaS and processors through API-based or CASB DLP where available.	• DLP policy set and coverage map • Discovery reports and inventory updates • DLP incident handling records
3.14	**1.** Enable access auditing on repositories holding sensitive data: file-server object access, database audit, application audit trails and cloud storage access logs. **2.** Capture read, modify, export and delete events, with user identity, time, source and object. **3.** Forward logs to a central SIEM, retain them in line with CERT-In and DPDP Rules expectations, and build alerts for unusual volumes or out-of-hours access.	• Audit configuration for sampled repositories • Sample sensitive data access logs in the SIEM • Alert rules and examples of investigations

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
An IG1 enterprise must run a documented data management process (3.1), know where its sensitive data is (3.2), restrict access on a need-to-know basis (3.3), keep data within defined minimum and maximum periods (3.4), dispose of it securely (3.5) and encrypt end-user devices holding sensitive data (3.6). For a 40-person firm this means a two-page data handling standard, a spreadsheet of sensitive data sets (client records, payroll, KYC documents), tidy share permissions, a retention table, a shredder and a certified e-waste vendor, and full-disk encryption turned on for every laptop. These six Safeguards also form a practical minimum for DPDP readiness.	IG2 adds a formal classification scheme (3.7), data flow documentation including service providers (3.8), encryption on removable media (3.9), in transit (3.10) and at rest (3.11), and segmentation of systems by data sensitivity (3.12). These suit organisations holding larger volumes of personal or regulated data, using several processors or operating in regulated sectors.	IG3 adds automated data loss prevention to discover and control sensitive data across the estate and at providers (3.13), and logging of access, changes and deletion of sensitive data (3.14). These are expected where data is a prime target, for example banks, large hospitals, insurers and organisations likely to be notified as Significant Data Fiduciaries under the DPDP Act.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 3.1 → 5.12 Classification of information; 5.33 Protection of records; 5.34 Privacy and protection of PII; 5.1 Policies for information security
- 3.2 → 5.9 Inventory of information and other associated assets; 5.34
- 3.3 → 5.15 Access control; 5.18 Access rights; 8.3 Information access restriction
- 3.4 → 5.33 Protection of records; 8.10 Information deletion
- 3.5 → 8.10 Information deletion; 7.10 Storage media; 7.14 Secure disposal or re-use of equipment
- 3.6 → 8.1 User endpoint devices; 8.24 Use of cryptography
- 3.7 → 5.12 Classification of information; 5.13 Labelling of information
- 3.8 → 5.14 Information transfer; 5.19 Information security in supplier relationships
- 3.9 → 7.10 Storage media; 8.24
- 3.10 → 5.14; 8.24; 8.20 Networks security
- 3.11 → 8.24 Use of cryptography
- 3.12 → 8.22 Segregation of networks; 8.31 Separation of development, test and production environments; 8.11 Data masking
- 3.13 → 8.12 Data leakage prevention
- 3.14 → 8.15 Logging; 8.16 Monitoring activities

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: ID.AM-07 (data inventories), ID.AM-03 (data flows), PR.DS-01 (data at rest), PR.DS-02 (data in transit), PR.AA-05 (access permissions), PR.PS-04 (log records), DE.CM-03 (personnel activity monitored) (Srida IT mapping)
- NIST SP 800-53 Rev. 5: RA-2 Security Categorization; SI-12 Information Management and Retention; MP-5 and MP-6 Media Transport and Sanitization; SC-8 Transmission Confidentiality; SC-28 Protection of Information at Rest; AC-3, AC-4, AC-6; AU-2 and AU-12
- ISO/IEC 27701 PIMS controls on records of processing, retention and disposal of PII
- PCI DSS v4.0.1: Requirements 3 (stored account data), 4 (transmission) and 9.4 (media) where card data is in scope

F India Regulatory Touchpoints

- DPDP Act 2023: s.8(5) reasonable security safeguards, s.8(6) breach intimation to the Board and affected Data Principals, s.8(7) erasure when the purpose is served or consent is withdrawn, and s.10 additional duties (DPIA, audit) for Significant Data Fiduciaries
- DPDP Rules 2025: r.6 examples of reasonable security safeguards (encryption, masking, tokenisation, access control, access logging and log retention), r.7 breach reporting including a detailed report to the Board, and r.8 erasure timelines with advance notice to the Data Principal
- RBI directions on storage of payment system data in India and RBI IT governance directions on data classification and encryption for banks and NBFCs; SEBI CSCRF data protection expectations for regulated entities
- Aadhaar Act 2016 and UIDAI regulations and circulars on storage, masking and vaulting of Aadhaar numbers; CERT-In Directions 2022 on log retention for 180 days

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Data is what attackers ultimately want, whether to sell, to ransom or to use for fraud. Modern ransomware groups steal data before encrypting systems and threaten to publish it, so a good backup no longer neutralises the attack. Insider misuse, mis-sent email, public cloud buckets, lost laptops and over-shared file folders cause a large share of breaches without any sophisticated attacker. Each of these is blunted by Control 3: data that is not kept cannot leak, data that is encrypted is useless when a laptop is stolen, data that only the right group can open is not exposed by a phished junior account, and access logs show what was taken.

Failure is now costly in India. The DPDP Act 2023 requires a Data Fiduciary to take reasonable security safeguards to prevent personal data breaches, to notify the Data Protection Board and affected individuals when a breach occurs, and to erase personal data when its purpose is served; the Schedule to the Act sets penalties that can reach ₹250 crore for failing to take reasonable security safeguards. The DPDP Rules 2025 describe what reasonable safeguards include, naming encryption, obfuscation, masking or tokenisation, access control, logging and monitoring of access, and retention of logs, and they set out how breaches must be reported. Most of these obligations take effect in phases after the Rules were notified in November 2025, so 2026–27 is the window in which organisations must make them operate.

Indian data also has sector overlays. RBI requires payment system data to be stored in India, UIDAI rules restrict how Aadhaar numbers are stored and displayed, SEBI and RBI expect data classification and encryption, and PMLA and tax laws require certain records to be kept for years. A data protection programme that ignores these will either delete records it was obliged to keep or keep personal data far beyond any justified purpose. Control 3 gives a structured way to reconcile them: one process, one inventory, one classification scheme and one retention schedule.

I Applicability

Every enterprise holds sensitive data, at least payroll and customer records, so Control 3 always applies. A 40-person Kochi CA firm meets IG1 with a short data handling standard, a list of the client files and KYC documents it holds and where, folder permissions by client team, a retention table that reflects professional and tax record-keeping rules, encrypted laptops and a shredding routine. SaaS-heavy organisations must remember that their data inventory, access permissions and retention settings live largely in provider consoles, and that service provider flows belong in 3.8; the shared-responsibility model leaves classification, access and retention with the customer. OT environments rarely hold personal data but do hold sensitive process recipes, drawings and quality records, which also deserve classification and protection. Where processing is outsourced, the enterprise remains the Data Fiduciary under the DPDP Act and must be able to show that its processors protect, retain and erase data as instructed.

J Implementation Guidance

1. Appoint an accountable owner for data protection (CISO with the DPO or privacy lead), and name data owners for each major data domain: customers, employees, finance, patients or clients, suppliers and intellectual property.
2. Write the data management standard and classification scheme together, so that each class has clear handling, retention and disposal rules, and add DPDP and sector tags.
3. Build the data inventory, starting with personal and other sensitive data, through owner workshops validated by discovery scans; link each data set to systems and processors.

4. Clean up access: remove open shares and public links, introduce role-based groups approved by data owners and schedule periodic re-certification.
5. Encrypt every end-user device that can hold sensitive data, with central key escrow, and decide policy for removable media.
6. Build the retention schedule, resolving DPDP erasure against statutory minimums, and configure retention in mail, file, database, backup and log systems.
7. Formalise disposal for digital data, media, paper and hardware, with certificates and processor deletion confirmations.
8. At IG2, document data flows, enforce encryption in transit and at rest with managed keys, and segment systems and non-production environments by sensitivity.
9. At IG3, deploy DLP in discovery mode, tune India-specific detectors, then enforce on high-risk channels; enable and centralise sensitive-data access logging with alerting.
0. Review the process, inventory, classification and flows annually and on significant change, and report metrics to management and, where relevant, to the DPDP compliance governance forum.

K Tools and Automation

- Data discovery and classification tools: scan file shares, endpoints, databases and cloud storage for personal and sensitive data, including Aadhaar, PAN and card patterns.
- DLP (endpoint, network, email and cloud/CASB): detects and blocks sensitive data leaving approved channels.
- Native full-disk encryption with MDM or directory key escrow (BitLocker, FileVault, LUKS) for end-user devices and removable media.
- Key management system or HSM: generates, stores and rotates keys for encryption at rest and tokenisation.
- Database activity monitoring and file access auditing feeding a SIEM (for example, Wazuh): records and alerts on sensitive data access.
- Records and retention management features in email, collaboration and storage platforms: enforce minimum and maximum retention.
- TLS and certificate scanning tools: find weak protocols and expiring certificates on services carrying sensitive data.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
Board / senior management	Approves the data protection policy and risk appetite and receives reports, including DPDP compliance status.
CISO	Owns the security controls in this Control: encryption, segmentation, DLP and logging.
Data Protection Officer / privacy lead	Owns DPDP alignment: inventory as record of processing, retention and erasure, breach notification readiness.
Data owners (business heads)	Classify their data, approve access, set retention and confirm disposal.
IT operations and cloud teams	Configure permissions, encryption, retention policies and log forwarding.
Legal / compliance	Interprets statutory retention minimums, sector rules and cross-border restrictions.
Service providers and processors	Protect, retain and delete data as instructed and confirm deletion at contract end.

M Documentation and Records

- Data management standard, including handling rules per class
- Data classification scheme and handling matrix with regulatory tags
- Data inventory or record of processing
- Retention schedule with minimum and maximum periods and legal basis
- Secure disposal procedure, disposal log and certificates of destruction
- Data flow diagrams including processors and cross-border transfers
- Cryptography and key management standard
- DLP policy set and incident handling procedure

- Logging standard for sensitive data access

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 9-2. Assessment testing procedures, Control 3

Test ID	Method	Testing procedure	Result
TP-C03-01	EXAMINE	3.1: Examine the data management standard and confirm it covers sensitivity, ownership, handling, retention limits and disposal; confirm approval by management and a review within the last 12 months or after the most recent significant change.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-02	INTERVIEW	3.1: Interview two data owners to confirm they know the data they own, the handling rules for it and how they approve access and exceptions.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-03	EXAMINE	3.2: Examine the data inventory and confirm sensitive and personal data sets are recorded with system, location, owner, purpose and retention rule, and that it was updated in the last 12 months.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-04	SAMPLE	3.2: Select 5–10 business processes (for example, payroll, customer onboarding, collections) and trace the personal data they use to inventory entries; separately run or review a discovery scan on two repositories to identify sensitive data absent from the inventory.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-05	INSPECT	3.3: Inspect permissions on a sample of 10 repositories holding sensitive data (file shares, cloud folders, databases, application roles). Identify broad grants, public links or individual exceptions, and confirm group membership was approved by the data owner.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-06	RE-PERFORM	3.3: Using a standard test account in a non-privileged role, attempt to open sensitive repositories outside that role and confirm access is denied.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-07	EXAMINE	3.4: Examine the retention schedule and confirm each data category has a minimum and a maximum period with a legal or business basis, and that conflicts between DPDP erasure and sector retention rules are resolved in writing.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-08	INSPECT	3.4: Inspect retention configurations in email, file storage, databases, backups and logs for a sample of categories and confirm they match the schedule; sample records to find any held beyond their maximum.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-09	SAMPLE	3.5: Select a sample of disposed assets and media from the last 12 months and trace each to a certificate of destruction or wiping record; sample processor contract exits to confirm deletion confirmations.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-10	OBSERVE	3.5: Observe paper and media disposal practice at one office, including secure bins and shredding, and confirm it follows the procedure for the class of data concerned.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-11	INSPECT	3.6: Inspect the MDM or endpoint encryption compliance report against the Control 1 asset register; sample 10 devices including laptops, mobile devices and contractor devices and confirm encryption is active and recovery keys are escrowed.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-12	EXAMINE	3.7: Examine the classification scheme for defined levels, criteria, handling rules and regulatory tags, review date and evidence that labels or handling rules are applied in practice.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C03-13	**SAMPLE**	3.7: Sample 10 documents or data sets and confirm their classification is correct under the scheme and that handling (location, sharing, encryption) matches the rules for that class.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-14	**EXAMINE**	3.8: Examine data flow diagrams for key processes and confirm they show service providers, cross-border transfers and protections, and were reviewed within the last 12 months or after significant change; trace one flow end to end with IT.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-15	**RE-PERFORM**	3.9: On a sample of endpoints, insert an unencrypted USB drive and confirm the device either blocks it or forces encryption before write; inspect the exception list for approved media.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-16	**RE-PERFORM**	3.10: Run a TLS configuration scan against externally and internally facing services that carry sensitive data and confirm only strong protocols and ciphers are accepted; check for clear-text protocols on sampled servers.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-17	**INSPECT**	3.11: Inspect encryption-at-rest settings for a sample of databases, storage volumes, object stores and backups holding sensitive data; inspect key management records for custodianship, access and rotation.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-18	**INSPECT**	3.12: Inspect the zone design and firewall or security group rules separating high-sensitivity systems; sample non-production databases to confirm sensitive data is masked or synthetic.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-19	**EXAMINE**	3.13: Examine DLP coverage (endpoints, email, web, cloud) against the asset register and the channel list; examine detection policies for India-specific identifiers and confirm discovery results update the data inventory.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-20	**RE-PERFORM**	3.13: Send test data containing synthetic Aadhaar-format and card-format numbers by email and upload to an unsanctioned cloud service, and confirm DLP detects or blocks it as designed.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-21	**INSPECT**	3.14: Inspect audit configuration on a sample of sensitive repositories and confirm read, modify and delete events are logged, forwarded to the SIEM and retained for the required period.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C03-22	**RE-PERFORM**	3.14: Access, modify and delete a test record in a sensitive repository and confirm the events appear in the SIEM with user, time and object, and that any relevant alert fires.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Build populations from the data inventory (data sets and repositories), the asset register (devices for encryption) and the retention schedule (categories). Stratify by classification, giving more weight to Restricted and personal data, and include at least one cloud and one service provider repository in each sample. For repository permissions use 10–15 items; for device encryption 10–25 devices including mobile and contractor devices; for disposal 10 items across media types; for retention 5–8 categories traced into system configurations. Where Safeguards carry an annual review, test the most recent cycle and any change-triggered review. Re-performance tests should use synthetic data only, never real personal data.

P Interview Questions

Interviewee	Question
DPO / privacy lead	Where is the most sensitive personal data held, and how do you know the inventory is complete?
DPO / privacy lead	How do you reconcile DPDP erasure duties with the record-keeping periods sector rules require?
Data owner	Who can see your data today, and when did you last confirm that list?
IT operations	How are laptops and removable media encrypted, and how do you find a device that is not?

Interviewee	Question
CISO	If a database of customer records were copied out tonight, what would detect it and what logs would show who did it?
Procurement / vendor manager	How do you confirm a processor has deleted our data at the end of a contract?

Q Technical and Process Verification

- A data management process, classification scheme and retention schedule exist, are approved and are reviewed on time.
- Sensitive and personal data is inventoried and linked to systems, owners and processors.
- Access to sensitive data is restricted to need-to-know groups and re-certified.
- Retention and disposal operate in systems and are evidenced.
- Encryption is in place on endpoints, removable media, in transit and at rest for the target IG.
- DLP and sensitive data access logging operate and are acted on (IG3).

R Expected Evidence

- Data management standard, classification scheme and retention schedule
- Data inventory or record of processing
- Repository permission reports and access review records
- Retention configurations and retention sweep reports
- Disposal log and certificates of destruction
- Endpoint and removable media encryption compliance reports
- TLS scan results and encryption-at-rest configuration
- Data flow diagrams and zone design
- DLP policies, incident records and sensitive data access logs

S Evaluation Criteria

Implemented

- Governance documents are current and reflect DPDP and sector requirements, and the inventory covers all sensitive data.
- Access, retention, disposal and encryption controls for the target IG operate and sampling shows few exceptions.
- Where IG3 is targeted, DLP and access logging produce alerts that are investigated.

Partially implemented

- Documents exist but the inventory or retention schedule is incomplete or not configured in systems.
- Encryption covers laptops but not mobile, removable media or databases required at the target IG.
- DLP runs in monitor-only mode without tuning or follow-up.

Not implemented

- No data management process or inventory of sensitive data.
- Sensitive data is broadly accessible and end-user devices are unencrypted.
- Data is kept indefinitely with no disposal records.

T Common Gaps and Findings

- Condition: customer KYC folders on the file server are readable by all domain users. Criteria: 3.3 requires need-to-know permissions. Effect: any compromised account exposes identity documents of all customers, creating a DPDP breach.
- Condition: the retention schedule lists minimum periods only. Criteria: 3.4 requires both minimum and maximum timelines. Effect: personal data is kept indefinitely, contrary to DPDP erasure duties and enlarging breach impact.
- Condition: 40% of field-staff phones have no passcode or encryption. Criteria: 3.6 requires encryption on end-user devices holding sensitive data. Effect: lost devices expose customer data and may trigger breach notification.
- Condition: production patient data is copied into the test environment unmasked. Criteria: 3.12 requires segmentation by sensitivity. Effect: weaker test controls expose health data.
- Condition: data flows to a cloud call-centre processor are not documented. Criteria: 3.8 requires documentation including service provider flows. Effect: the enterprise cannot show where personal data goes or enforce deletion.
- Condition: database access to the core system is not audited. Criteria: 3.14 requires logging of sensitive data access. Effect: insider misuse cannot be detected or investigated.

U Remediation Guidance

- Replace broad grants with data-owner-approved role groups and run quarterly access reviews on sensitive repositories.
- Add maximum retention periods with triggers, configure automatic deletion or archival, and document conflicts resolved with legal.
- Enforce device encryption and passcodes through MDM, blocking non-compliant devices from corporate data.
- Introduce masking or synthetic data for non-production and restrict copies of production data.
- Document all processor flows, update contracts with deletion and breach notification clauses, and obtain deletion confirmations.
- Enable database audit and forward to the SIEM with alerts for bulk exports and out-of-hours access.

V Monitoring Metrics

- Percentage of sensitive data sets in the inventory with a named owner and retention rule (target 100%).
- Percentage of end-user devices holding sensitive data that are encrypted (target 100%).
- Number of sensitive repositories with broad or public access grants (target zero).
- Volume or count of records held beyond maximum retention, trended quarterly.
- DLP high-severity incidents per month and median time to close (IG3).

W Related Controls and Maturity Indicators

- 1.1 and 2.1 (assets and software holding the data)
- 4.1 (secure configuration supports encryption and permissions)
- 5.x and 6.x (account and access management underpin 3.3)
- 8.2 and 8.10 (log collection and retention for 3.14)
- 11.3 (protect recovery data)
- 12.2 and 12.8 (network design for segmentation)
- 14.4 (awareness of data handling)
- 15.4 (service provider contracts for 3.8)
- 17.x (incident response for data breaches and DPDP notification)

Initial	Defined	Managed	Optimised
Data is stored wherever users choose; no inventory, classification or retention rules exist, and encryption is accidental.	A data management process, classification scheme, inventory and retention schedule are documented and owners are named.	Access, retention, disposal and encryption are configured and monitored; flows and segmentation are documented and reviewed; metrics are reported.	Discovery and DLP keep the inventory current automatically, access to sensitive data is logged and analysed, and data protection evidence directly supports DPDP accountability and audits.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A Hyderabad hospital chain with six hospitals and 3,500 staff prepared for the DPDP Rules commencement by using Control 3 as its technical plan. A first workshop with clinical, finance and HR heads produced an inventory of 42 data sets. It found patient records held in the hospital information system, a radiology archive, a cloud-based teleconsultation platform, shared folders of discharge summaries and personal WhatsApp groups used by doctors to share images.

The chain adopted a four-level scheme (Public, Internal, Confidential, Restricted) with tags for health data, children's data and Aadhaar numbers. Patient clinical data and Aadhaar-linked insurance claims were classed Restricted. A retention schedule set minimum periods based on medical record and tax rules identified by its legal team, with a maximum period after which records are archived offline or destroyed. Conflicts were written down and approved by the medical director and DPO.

Access to the shared discharge folders was narrowed from all staff to ward-based groups. All laptops and the tablets used on wards were encrypted through MDM, and USB storage was blocked except for encrypted drives issued to the radiology team. The IT team enabled TLS 1.2 or higher on the teleconsultation interface, turned on database encryption for the hospital information system and moved the test environment to synthetic data.

In the following year, having been told it might be notified as a Significant Data Fiduciary, the chain deployed DLP in discovery mode, which found unmasked Aadhaar numbers in 1,800 insurance documents. These were masked, and database audit logs for the hospital information system were sent to the SIEM with alerts for bulk exports. The next internal audit rated Safeguards 3.1–3.12 as implemented and 3.13–3.14 as partially implemented.

WP-C03: use the workpaper format shown in Appendix H.

CHAPTER 10 · CIS CONTROL 4

Secure Configuration of Enterprise Assets and Software

CIS CONTROL 4 · 12 SAFEGUARDS · 7 IN IG1

Secure Configuration of Enterprise Assets and Software

CIS Controls v8.1 · titles quoted verbatim | WP-C04

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 4 — Secure Configuration of Enterprise Assets and Software

Control 4 is about turning equipment and software from the state in which they arrive into a state the enterprise has deliberately chosen, and then keeping them there. It applies to laptops, desktops, phones, servers, network devices, IoT and operational devices, cloud services, operating systems and applications. The Control has two halves. The first is governance: a documented, owned and reviewed process for hardening ordinary assets (4.1) and network infrastructure (4.2). The second is a set of specific technical settings that almost every enterprise needs: screen locks, host firewalls, secure management channels, removal of default accounts and surplus services, trusted DNS, lockout after failed sign-ins, remote wipe and separation of work data on mobiles. Secure configuration is not a one-off build activity. Settings drift when software is updated, when an engineer loosens something to fix a problem, or when a new device is added in a hurry, so the Control expects continuous comparison of the live estate against the approved baseline.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 10-1. Safeguards of CIS Control 4, Secure Configuration of Enterprise Assets and Software

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
4.1	**“Establish and Maintain a Secure Configuration Process”**	Documentation	Govern	**IG1**	Keep a written, owned process that says how every class of enterprise asset (laptops, phones, servers, IoT and non-computing devices) and every operating system and application is brought to an approved hardened state, kept there and changed under control. The document is reviewed at least once a year and again whenever a material change, such as a cloud move or a merger, affects it.
4.2	**“Establish and Maintain a Secure Configuration Process for Network Infrastructure”**	Documentation	Govern	**IG1**	Keep an equivalent written process for routers, switches, firewalls, wireless controllers, VPN concentrators, load balancers and cloud network constructs, covering hardening, configuration backups, change approval and periodic comparison against the approved build. Review it annually and after significant network change.
4.3	**“Configure Automatic Session Locking on Enterprise Assets”**	Devices	Protect	**IG1**	Make every enterprise asset lock its session automatically after a period of inactivity, so an unattended screen cannot be used by someone else. The idle period is capped at 15 minutes for general-purpose operating systems and 2 minutes for mobile phones and tablets; shorter is acceptable.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
4.4	**“Implement and Manage a Firewall on Servers”**	Devices	Protect	IG1	Run and actively manage a firewall on each server wherever the platform supports one, whether that is the host operating system firewall, a hypervisor or cloud virtual firewall, or an agent-based firewall. Rules should allow only the traffic the server's role needs.
4.5	**“Implement and Manage a Firewall on End-User Devices”**	Devices	Protect	IG1	Run a host firewall or port-filtering capability on laptops and desktops that denies inbound traffic by default and allows only explicitly approved services and ports. The setting must hold whether the device is in the office, at home or on public Wi-Fi.
4.6	**“Securely Manage Enterprise Assets and Software”**	Devices	Protect	IG1	Administer assets and software in a controlled, repeatable and secure way: prefer configuration held as version-controlled code or templates, and reach management interfaces only over encrypted protocols such as SSH and HTTPS. Clear-text management protocols like Telnet or plain HTTP are not used unless there is a documented operational need with compensating controls.
4.7	**“Manage Default Accounts on Enterprise Assets and Software”**	Users	Protect	IG1	Deal with every account that ships pre-built with a product, such as root, built-in administrator, guest or vendor support logins, so that it cannot be used as delivered. Typical treatments are disabling it, renaming and locking it, or replacing its credential with a strong unique secret held in a vault.
4.8	**“Uninstall or Disable Unnecessary Services on Enterprise Assets and Software”**	Devices	Protect	IG2	Remove or switch off services, features, modules and listeners that an asset or application does not need for its business role, such as an unused file share, a sample web module or a legacy protocol. Fewer running components means fewer ways in.
4.9	**“Configure Trusted DNS Servers on Enterprise Assets”**	Devices	Protect	IG2	Point enterprise assets and network infrastructure at DNS resolvers the enterprise controls or has deliberately chosen as reputable, so name resolution cannot be silently redirected. Devices should not pick up arbitrary resolvers from untrusted networks where this can be prevented.
4.10	**“Enforce Automatic Device Lockout on Portable End-User Devices”**	Devices	Protect	IG2	Have portable devices lock themselves (or wipe or escalate delay) after a set number of failed local sign-in attempts, where the platform supports it. The threshold is no more than 20 attempts for laptops and no more than 10 for tablets and smartphones.
4.11	**“Enforce Remote Wipe Capability on Portable End-User Devices”**	Data	Protect	IG2	Be able to erase enterprise data remotely from enterprise-owned portable devices when that is the right response, for example when a device is lost or stolen or when its user leaves the enterprise. The capability must be enrolled before it is needed.
4.12	**“Separate Enterprise Workspaces on Mobile End-User Devices”**	Data	Protect	IG3	On mobile devices, keep enterprise apps and data in a managed container or work profile that is separated from the user's personal apps and data, where the platform supports it. This protects enterprise data without taking control of the whole personal device.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
4.1	1. Pick a reference baseline for each platform in the asset inventory (for example a CIS Benchmark level, a vendor hardening guide or an internal standard) and record any deliberate deviations with a reason and an approver. 2. Describe the lifecycle in the process: how a golden image or template is built, how it is applied at build time, how drift is detected and how a change to the baseline is requested, tested and approved. 3. Assign an owner per platform, store the baselines under version control and diarise the annual review plus triggers for out-of-cycle review. 4. Link the process to Control 1 (which assets exist) and Control 2 (which software is authorised) so that no asset class falls outside it.	• Approved secure configuration standard with version history and the last annual review record • Baseline files or images per platform with recorded deviations • Change tickets showing baseline changes passed through approval
4.2	1. Write a network device hardening standard covering management-plane access, logging, NTP, SNMP versions, banner, unused ports, and routing protocol authentication. 2. Hold the approved running configuration of each device in a repository and compare live configurations against it on a schedule, raising tickets for unexplained differences. 3. Require change approval and a back-out plan for any configuration change to network devices, including changes made by an MSP or ISP. 4. Include cloud security groups, virtual network rules and SD-WAN policies in scope, not only physical boxes.	• Network device hardening standard with annual review evidence • Configuration backup and comparison reports • Sample of approved network change records
4.3	1. Set the lock timer centrally through directory group policy, MDM or configuration management rather than relying on users. 2. Apply the same rule to servers' interactive consoles, jump hosts and virtual desktop sessions, not only laptops. 3. Document exceptions such as shared display screens or clinical workstations and apply compensating measures (kiosk mode, proximity badges, physical supervision).	• Policy or MDM profile showing the idle-lock value per platform • Compliance report from the management tool showing devices that meet or miss the setting
4.4	1. Define a rule set per server role (web, database, file, domain controller) that allows only required ports and sources. 2. Enforce the firewall state centrally and alert when it is switched off or a broad allow-any rule appears. 3. Review server firewall rules at least annually and when an application is retired, removing stale entries.	• Firewall state report across the server estate • Approved rule sets per server role with review dates

Safeguard	Practical steps	Evidence
4.5	1. Enable the operating system firewall on all profiles with an inbound default-deny stance and a short list of approved exceptions. 2. Lock the setting so users cannot disable it, using MDM or group policy. 3. Monitor compliance through the endpoint management console and investigate devices that report the firewall as off.	• Endpoint firewall policy export showing default-deny inbound • Device compliance report for firewall state
4.6	1. Inventory management interfaces (SSH, RDP, web consoles, SNMP, IPMI/iLO-type out-of-band controllers) and disable clear-text variants. 2. Move repeatable builds (cloud resources, server roles, network templates) into code repositories with peer review before deployment. 3. Restrict management interfaces to a management network or jump host and log all administrative sessions.	• Scan output showing no Telnet, plain HTTP or SNMPv1/v2c management listeners, or approved exceptions • Repository history for infrastructure code with review approvals
4.7	1. Build a checklist of known default accounts per product class (operating systems, databases, network devices, printers, CCTV, IoT, SaaS admin consoles). 2. Make default account treatment a mandatory step in the build and commissioning checklist, signed off before go-live. 3. Scan periodically for default credentials using authenticated vulnerability scanning and fix findings as high priority.	• Build checklist showing default account handling • Scanner results for default credential checks • Vault record for break-glass use of any retained built-in account
4.8	1. Define the minimum service set for each server role and endpoint build as part of the baseline. 2. Compare running services and listening ports against that set using configuration assessment or network scanning, and raise tickets for differences. 3. Remove sample applications, default web pages and demo databases at commissioning.	• Role baselines listing permitted services • Configuration assessment or port scan reports with remediation tickets
4.9	1. Decide the approved resolvers (internal resolvers forwarding to a filtering or reputable external service) and document them. 2. Push resolver settings through DHCP, group policy, MDM or always-on VPN for roaming devices, and block outbound DNS to unapproved resolvers at the perimeter. 3. Monitor for devices or applications using other resolvers, including encrypted DNS configured inside browsers.	• Network and endpoint configuration showing approved resolvers • Firewall rules restricting outbound port 53 and encrypted DNS to approved resolvers
4.10	1. Configure the failed-attempt threshold in MDM or endpoint policy for each portable platform. 2. Pair the setting with full-disk encryption so the lockout cannot be bypassed by removing the storage. 3. Test on a sample device and record the behaviour in the build sign-off.	• MDM or policy export showing the threshold per platform • Test record from a sample device

Safeguard	Practical steps	Evidence
4.11	**1.** Enrol all enterprise-owned laptops, phones and tablets in MDM with remote wipe or remote lock-and-wipe enabled. **2.** Write a lost-device and leaver procedure saying who may authorise a wipe, how fast, and how the action is recorded. **3.** Run a periodic test wipe on a spare device and reconcile the MDM enrolment list against the asset inventory.	• MDM enrolment coverage report reconciled to the asset inventory • Wipe action logs for lost devices and leavers • Lost-device procedure
4.12	**1.** Choose a separation model per platform (work profile, managed apps with data-transfer restrictions, or user enrolment) and document it. **2.** Block copy, paste and sharing from managed to unmanaged apps and require enterprise apps to run only inside the managed space. **3.** Enable selective wipe of the enterprise workspace for bring-your-own devices.	• MDM configuration for work profiles or managed-app policies • Test result showing data cannot move from work to personal space

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
IG1 contains seven Safeguards here: 4.1 and 4.2 (documented secure configuration processes for assets and for network devices), 4.3 (automatic session lock), 4.4 and 4.5 (firewalls on servers and on end-user devices), 4.6 (secure management of assets and software) and 4.7 (default accounts dealt with). For a small firm this can be achieved with the built-in management features of a typical office productivity suite and the operating system: a one-page hardening standard per platform, screen-lock and firewall policies pushed from the device management console, changed router and printer passwords, and HTTPS-only access to device admin pages. A 40-person firm does not need a configuration management database to meet IG1, but it does need to be able to show what its standard is and that its devices follow it.	IG2 adds four Safeguards: 4.8 (unnecessary services removed or disabled), 4.9 (trusted DNS resolvers), 4.10 (lock-out after failed local sign-in on portable devices) and 4.11 (remote wipe). These reflect a larger, more mobile workforce and a more varied estate where unmanaged services and lost devices become a real exposure. IG2 enterprises are also expected to apply the IG1 Safeguards with tooling that measures drift across the estate rather than relying on spot checks.	IG3 adds one Safeguard, 4.12 (separate enterprise workspaces on mobile devices). It is aimed at enterprises handling sensitive data on phones and tablets, often under bring-your-own-device arrangements, who must protect enterprise data without managing the whole personal device. IG3 enterprises would also be expected to automate baseline enforcement and drift remediation broadly, typically through infrastructure-as-code and continuous configuration assessment.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 4.1 → 8.9 Configuration management; 5.37 Documented operating procedures; 8.32 Change management
- 4.2 → 8.9 Configuration management; 8.20 Networks security; 8.32 Change management
- 4.3 → 8.1 User endpoint devices; 7.7 Clear desk and clear screen
- 4.4 → 8.20 Networks security; 8.22 Segregation of networks
- 4.5 → 8.1 User endpoint devices; 8.20 Networks security
- 4.6 → 8.9 Configuration management; 8.2 Privileged access rights; 8.24 Use of cryptography
- 4.7 → 5.17 Authentication information; 8.2 Privileged access rights; 8.9 Configuration management
- 4.8 → 8.9 Configuration management; 8.19 Installation of software on operational systems
- 4.9 → 8.20 Networks security; 8.21 Security of network services
- 4.10 → 8.1 User endpoint devices; 8.5 Secure authentication
- 4.11 → 8.1 User endpoint devices; 7.9 Security of assets off-premises; 8.10 Information deletion
- 4.12 → 8.1 User endpoint devices; 6.7 Remote working
- Clauses 6.1.3 (risk treatment, Statement of Applicability) and 8.1 (operational planning and control) frame the baseline as a documented treatment

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: PR.PS-01 (configuration management practices established and applied) for 4.1, 4.2, 4.6–4.8; PR.IR-01 (networks and environments protected from unauthorised logical access) for 4.4, 4.5, 4.9; PR.AA-03 for 4.3 and 4.10; PR.DS-01 for 4.11 and 4.12 (Srida IT mapping)
- NIST SP 800-53 Rev. 5: CM family (CM-2 baseline configuration, CM-6 configuration settings, CM-7 least functionality), AC-11 device lock, AC-7 unsuccessful logon attempts, SC-7 boundary protection, MP-6 and AC-19 for mobile devices
- CIS Benchmarks and CIS Build Kits as baseline sources for many platforms

F India Regulatory Touchpoints

- CERT-In Directions of 28 April 2022: synchronisation of system clocks to the specified NTP sources and enablement of logs on ICT systems are, in practice, items in the secure configuration baseline; the 180-day log retention depends on correct log settings
- RBI cyber security framework and IT governance directions for banks and NBFCs: expectations of documented secure configuration standards, hardening of servers and network devices and periodic configuration review
- SEBI CSCRF (2024): configuration management and hardening expectations for regulated entities, with periodic review and audit according to the entity's category
- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6: reasonable security safeguards for personal data; hardened, encrypted and wipe-capable endpoints are a common way to evidence this. Mapping is not compliance

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Products are shipped to work first time for the largest number of buyers. That usually means open ports, sample content, guest or vendor accounts with published passwords, permissive sharing and old protocols left on for compatibility. Attackers know these defaults well; automated scanners look for exposed management pages, Telnet on routers, unchanged CCTV passwords and RDP left open on cloud servers within minutes of a host appearing on the internet. Ransomware operators routinely move laterally using file shares and remote management services that were never needed on the machines where they were found. A hardened baseline closes most of these doors before any detection tool is needed.

Failure is usually quiet. A single change made during an outage, such as disabling a server firewall to test connectivity, can remain for years. Without a baseline and drift monitoring, nobody notices until an incident investigation finds it. Weak configuration also undermines other Controls: patching does not help if an unpatched legacy service is reachable that should have been removed, and logging cannot be relied on if device clocks and log settings are not part of the standard build.

In India the issue is sharpened by a large installed base of small-office routers, CCTV recorders and biometric attendance devices that are often installed by local integrators with factory credentials, and by heavy use of cloud and managed service providers whose shared-responsibility boundaries are poorly understood by smaller customers. Regulators expect a documented baseline: the CERT-In Directions require time synchronisation and log enablement that are, in practice, configuration items, and sector regulators such as RBI and SEBI expect secure configuration standards and periodic configuration review in their cyber security frameworks.

I Applicability

Every enterprise has devices and software that arrive with defaults, so this Control applies universally. A small firm with twenty laptops and a broadband router can meet IG1 with the device management features already in its productivity suite and a short written standard; the priority items are screen lock, firewall on, router and printer passwords changed, and admin pages reached only over HTTPS. Cloud and SaaS-heavy enterprises should treat tenant security settings, cloud security groups and infrastructure templates as configuration items under the same process, and should read the provider's shared-responsibility model carefully because many PaaS services leave hardening of the hosted application to the customer. Enterprises with OT, such as manufacturing plants, must adapt: PLC programming stations and HMIs often cannot run host firewalls or short screen locks, so the baseline should record the exception and rely on network segmentation, physical control and vendor-approved hardening. Where an MSP or system integrator builds and runs systems, the enterprise still owns the baseline; contracts should require the MSP to apply it, report drift and change default credentials at installation.

J Implementation Guidance

1. Start from the asset and software inventories (Controls 1 and 2) and group assets into platforms that share a baseline: Windows endpoints, macOS, Linux servers, mobile, network devices, cloud tenant, key SaaS, IoT/OT.
2. Select a reference baseline for each platform, adopt it at a sensible level, and record every deliberate deviation with a business reason and approver. Do not try to apply every hardening item at once; begin with a profile that will not break business applications and tighten later.
3. Write the secure configuration process (4.1) and the network equivalent (4.2): ownership, build, deviation approval, drift detection, change control and annual review.
4. Build golden images, templates or infrastructure code that embed the baseline, so new assets are compliant from day one, and retire hand-built servers over time.
5. Push the high-value technical settings centrally: idle lock (4.3), host firewalls (4.4, 4.5), encrypted management only (4.6), default accounts disabled or vaulted (4.7), surplus services removed (4.8), approved DNS (4.9), failed-attempt lockout (4.10), MDM enrolment with remote wipe (4.11) and work profiles where needed (4.12).
6. Deploy a means of measuring compliance continuously, such as configuration assessment in the endpoint or vulnerability management tool, and report the percentage of assets meeting the baseline by platform.
7. Route every baseline change and every exception through change management, with an expiry date for exceptions.
8. Add configuration checks to commissioning: no device, including CCTV, printers and IoT installed by contractors, goes live until defaults are changed and the checklist is signed.
9. Review drift reports monthly, fix or approve each difference, and carry out the formal annual review of both processes, recording the outcome.

K Tools and Automation

- Endpoint and mobile device management (MDM/UEM) to push lock, firewall, lockout, encryption, remote wipe and work-profile settings and report compliance
- Configuration assessment or compliance scanning (including authenticated scanning in OpenVAS/Greenbone-type scanners or agent-based tools such as Wazuh SCA) to compare live settings with the baseline
- Infrastructure-as-code and configuration management tools with a version-controlled repository, to define builds as reviewed code
- Network configuration management tools that back up device configurations and highlight changes against the approved version
- Privileged access management or a password vault to hold any retained built-in account credentials
- Protective DNS resolvers and perimeter firewall rules to enforce approved name resolution
- osquery or similar endpoint query tools to check settings and listening services across the estate

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
CISO / Head of Information Security	Owns the secure configuration policy, approves baselines and significant deviations, and reports compliance to management
Platform owners (endpoint, server, network, cloud)	Maintain the baseline for their platform, apply it through tooling, remediate drift and propose changes
Change Advisory Board or change manager	Approves baseline changes and time-bound exceptions and checks back-out plans
IT operations / MSP	Builds assets from approved images, commissions devices with defaults changed and keeps the management tools running
Internal audit or assessor	Tests the design and operation of the process and samples assets against the baseline
Asset owners / business heads	Accept residual risk for exceptions affecting their systems

M Documentation and Records

- Secure configuration policy and process (assets) and network device configuration process, with review history
- Platform baselines with recorded deviations and approvers
- Golden image and template register with version numbers
- Exception register with expiry dates and compensating controls
- Commissioning checklist including default account and service removal
- Lost or stolen device and leaver device-wipe procedure
- Drift and compliance reports with remediation tickets

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 10-2. Assessment testing procedures, Control 4

Test ID	Method	Testing procedure	Result
TP-C04-01	EXAMINE	4.1: Examine the documented secure configuration process for enterprise assets and software. Confirm that it covers every asset class in the Control 1 inventory (end-user, portable and mobile devices, servers, IoT and non-computing devices) and the operating systems and applications in the Control 2 inventory, names an owner per platform, references a baseline source, and describes build, deviation approval, drift detection and change control.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-02	INSPECT	4.1: Inspect the document's version history and review records. Confirm that it was reviewed within the last twelve months and also after any significant change in the period (for example cloud migration or new platform adoption). Select two baseline changes from the change log and confirm that each passed through approval and was reflected in the baseline file or image.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-03	EXAMINE	4.2: Examine the network infrastructure configuration process and hardening standard. Confirm coverage of routers, switches, firewalls, wireless, VPN, load balancers and cloud network controls, and that it addresses management access, logging, time synchronisation, SNMP version, unused ports and configuration backup. Confirm annual review evidence and review after significant network change.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-04	SAMPLE	4.2: Select a sample of network devices (see sampling) and compare each running configuration with the approved stored configuration and with the hardening standard. Select a sample of network changes over the review period and confirm approval, back-out plan and post-change configuration backup.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-05	INSPECT	4.3: Inspect the group policy, MDM profiles or configuration management settings for session locking on each platform. Confirm the idle timeout does not exceed 15 minutes on general-purpose operating systems and 2 minutes on mobile devices, and that users cannot extend it.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-06	OBSERVE	4.3: For a sample of endpoints, servers with interactive consoles and mobile devices, observe the device left idle (or inspect the effective local setting) and confirm it locks within the configured period. Obtain the management tool's compliance report and confirm the proportion of non-compliant devices and their follow-up.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-07	SAMPLE	4.4: From the server inventory, select a sample across on-premises, virtual and cloud servers and inspect the firewall state and rule set for each. Confirm the firewall is active where supported, rules match the approved role-based set, and no broad allow-any inbound rules exist without an approved exception. Confirm rules were reviewed in the last year.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C04-08	**INSPECT**	4.5: Inspect the endpoint firewall policy and a sample of end-user devices. Confirm the firewall is on for all network profiles, inbound traffic is denied by default with only approved exceptions, and users cannot switch it off. Review the compliance report for devices reporting the firewall disabled during the period and the action taken.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-09	**RE-PERFORM**	4.6: Re-perform a scan of management interfaces on a sample of servers, network devices, printers, storage and out-of-band controllers. Confirm that management is available only over encrypted protocols (for example SSH, HTTPS, SNMPv3) and that Telnet, plain HTTP and other clear-text management services are disabled, or are covered by an approved exception with compensating controls.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-10	**EXAMINE**	4.6: Examine how repeatable builds are managed. Where infrastructure-as-code or templates are used, select a sample of recent changes and confirm they were version-controlled and peer-reviewed before deployment. Confirm management interfaces are restricted to a management network or jump host and administrative sessions are logged.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-11	**SAMPLE**	4.7: Select a sample of assets across classes, including IoT, CCTV, printers, databases, network devices and SaaS admin consoles. For each, confirm that built-in and vendor default accounts are disabled, made unusable, or have had the default credential replaced with a unique secret held in a vault. Review the latest authenticated scan for default-credential findings and confirm remediation.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-12	**INSPECT**	4.8: Inspect the permitted-service list for a sample of server roles and endpoint builds. Compare running services and listening ports on sampled assets (from configuration assessment or a port scan) with the permitted list, and confirm that unexplained services were removed or approved. Confirm sample content and default web pages are absent from sampled web servers.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-13	**INSPECT**	4.9: Inspect DHCP scopes, network device settings, endpoint and MDM configuration and VPN profiles to confirm assets use the approved enterprise or reputable resolvers. Inspect perimeter firewall rules to confirm that outbound DNS and known encrypted DNS endpoints are restricted to approved resolvers, and test from a sample endpoint that an unapproved resolver cannot be reached.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-14	**INSPECT**	4.10: Inspect MDM or endpoint policy for portable devices and confirm the failed local authentication threshold is set at no more than 20 attempts on laptops and no more than 10 on tablets and smartphones, where supported. For one laptop and one mobile device, observe or review a test record showing the lockout triggers.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-15	**SAMPLE**	4.11: Reconcile the MDM enrolment list with the asset inventory of enterprise-owned portable devices and confirm remote wipe is enabled. Select a sample of lost or stolen device reports and leavers with enterprise devices during the period and confirm a wipe (or documented alternative) was authorised and executed within the procedure's timescale.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-16	**RE-PERFORM**	4.12: Inspect the MDM configuration for work profiles or managed-app separation on mobile devices. On a sample enrolled device, re-perform an attempt to copy or share enterprise data into a personal app and confirm it is blocked, and confirm selective wipe of the work space is available.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C04-17	**INTERVIEW**	4.1: Interview platform owners and the change manager to confirm how drift is detected and handled, how often drift reports are reviewed, and how exceptions are approved and expired. Corroborate answers with a sample of drift reports and the exception register.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Use the review period agreed in the engagement, usually twelve months. Automated settings (screen lock, firewall state, lockout threshold, DNS settings) are tested by inspecting the policy once and then the tool's compliance report for the whole population, supported by a small observation sample of 5–10 devices per platform to confirm the report reflects reality. Where no central report exists, sample 25 endpoints, or all if fewer, spread across sites and device types. For servers sample 10–25 across on-premises, virtual and cloud, weighted towards internet-facing and critical systems. For network devices sample 5–15, always including the internet edge firewall and core switch. For default accounts and services include non-traditional assets (CCTV, printers, biometric devices, OT HMIs) because they are where defaults survive. For changes, sample 10–25 baseline or network changes across the period. For lost devices and leavers, test all cases if fewer than 15, otherwise 15. Extend the sample when an exception is found, and record the source, date and completeness check of each population.

P Interview Questions

Interviewee	Question
CISO	Which baseline sources have you adopted for each platform, and who approved the deviations from them?
Endpoint platform owner	How would you know if a laptop's firewall or screen lock was switched off, and how quickly would that be corrected?
Network engineer or MSP	When you last changed a firewall rule in an emergency, how was it recorded and reconciled to the approved configuration?
Facilities or IoT owner	Who installed the CCTV recorders and access-control panels, and how did you confirm their factory passwords were changed?
Service desk lead	Walk me through the last lost phone or laptop: who authorised the wipe and how long did it take?
Cloud engineer	How are cloud security groups and tenant settings controlled, and can anyone change them outside the code pipeline?

Q Technical and Process Verification

- Baselines exist for every platform in the inventory and are traceable to a source with approved deviations
- Compliance reports cover the full population, not a subset of managed devices
- Live configurations on sampled assets match the policy shown on paper
- Default credentials and clear-text management protocols are absent from sampled assets, including IoT and OT
- Exceptions have owners, compensating controls and expiry dates and are not simply permanent
- Annual and event-driven review of both processes is evidenced

R Expected Evidence

- Secure configuration process and network configuration process with review records
- Platform baselines and deviation registers
- MDM and group policy exports for lock, firewall, lockout, wipe and work-profile settings
- Configuration compliance and drift reports with remediation tickets
- Network configuration backups and comparison reports
- Authenticated scan results covering default credentials and services
- Management-interface scan results
- Lost-device and leaver wipe logs
- Change records for baseline and network changes

S Evaluation Criteria

Implemented

- A current, reviewed process and platform baselines exist, and tooling shows high compliance (for example 95% or more) across the whole population with drift handled
- Sampled assets, including IoT and network devices, match the baseline with no default credentials or clear-text management
- All IG-relevant technical settings are enforced centrally and tested

Partially implemented

- A process exists but has not been reviewed in the last year or omits an asset class such as network devices, cloud or IoT
- Settings are enforced on most endpoints but servers, mobiles or remote devices fall outside management
- Drift is detected but not consistently remediated or exceptions have no expiry

Not implemented

- No documented baseline; builds depend on individual engineers
- Firewalls, screen locks or default credentials are found unmanaged on a material share of sampled assets
- No ability to wipe or track enterprise portable devices

T Common Gaps and Findings

- Condition: Twelve CCTV recorders and four biometric attendance terminals still use the installer's default admin password. Criteria: 4.7 requires default accounts to be disabled or made unusable. Effect: Anyone on the network, or on the internet where ports are forwarded, can take control of devices that record sensitive premises footage.
- Condition: The secure configuration standard was last reviewed 26 months ago and does not cover the cloud tenant. Criteria: 4.1 requires annual review and coverage of all asset classes. Effect: Cloud resources are built without a reference baseline and drift is not measured.
- Condition: Server firewalls are disabled on 9 of 20 sampled servers 'for performance'. Criteria: 4.4 requires server firewalls where supported. Effect: Lateral movement between servers is unrestricted inside the data centre VLAN.
- Condition: Core switches and the edge firewall are managed over Telnet and HTTP from the user network. Criteria: 4.6 requires encrypted management protocols. Effect: Administrator credentials can be captured on the network.
- Condition: 31% of field-sales phones are not enrolled in MDM. Criteria: 4.11 requires remote wipe on enterprise portable devices. Effect: Customer data on lost phones cannot be erased, creating a possible personal data breach.
- Condition: Idle lock is set to 30 minutes on all Windows laptops. Criteria: 4.3 caps the period at 15 minutes. Effect: Unattended laptops in shared spaces remain usable for longer than accepted.

U Remediation Guidance

- Change all default credentials on IoT, CCTV and biometric devices within 30 days, vault the new secrets and add credential change to the integrator acceptance checklist.
- Revise and re-approve the secure configuration standard, add cloud and SaaS baselines, and diarise the next annual review.
- Re-enable server firewalls with role-based rules, starting with domain controllers and database servers, and alert on firewall state changes.
- Move network device management to SSH and HTTPS on a dedicated management VLAN reachable only from a jump host.
- Enrol all enterprise phones in MDM with remote wipe, and block mail and app access from unenrolled devices.
- Reduce idle lock to 10–15 minutes through central policy and communicate the change to users.

V Monitoring Metrics

- Percentage of assets, by platform, compliant with the approved baseline (target at least 95%)
- Number of open drift items older than 30 days
- Number of assets with default credentials found by authenticated scanning (target zero)
- Percentage of enterprise portable devices enrolled in MDM with remote wipe (target 100%)
- Number of approved configuration exceptions past their expiry date (target zero)

W Related Controls and Maturity Indicators

- Control 1 (asset inventory defines scope)
- Control 2 (authorised software)
- 5.4 and 6.5 (administrator accounts and MFA for administration)

- Control 7 (vulnerability management, which detects configuration weaknesses)
- 8.4 (time synchronisation as a configuration item)
- Control 12 (network infrastructure management)
- 3.6 (encryption of data on end-user devices)

Initial	Defined	Managed	Optimised
Devices are built by hand from the vendor default; some settings are changed by experienced staff but nothing is written down or measured.	A documented process and platform baselines exist, are owned and reviewed annually, and the main IG1 settings are pushed through central policy.	Compliance is measured across the whole estate, drift is reported monthly and remediated, exceptions expire, and new assets are built from approved images or templates.	Baselines are held as code, enforced automatically with self-healing of drift, tested in a pipeline before release, and refined from incident and threat intelligence.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

Fictional scenario — a Chennai auto-parts maker with OT. The company employs 850 people across a machining plant, a warehouse and a small head office. Its IT is run by a four-person team and an MSP; the plant network hosts PLC programming laptops, HMIs and a historian server installed by the automation vendor. A Srida IT assessment found no written baseline, Windows laptops with a 60-minute screen lock, the warehouse Wi-Fi controller and three CCTV recorders still using factory passwords, Telnet enabled on two core switches, and the historian server running a file share and remote desktop open to the whole office network.

Over six months the company adopted CIS Benchmark level 1 as the starting point for Windows and Linux, wrote a two-part secure configuration standard (assets and network) with recorded deviations, and gave the MSP a contractual duty to report drift monthly. Laptop policies now enforce a 10-minute lock, firewall on with inbound deny, and a lockout after 10 failed attempts. Network devices moved to SSH and HTTPS on a management VLAN. Default accounts on CCTV, Wi-Fi and printers were changed and the credentials vaulted. For the OT zone, where the vendor would not support host firewalls on HMIs, the standard records an exception with compensating controls: a firewall between IT and OT, removable media control and supervised engineering access. The historian's file share was removed.

At the follow-up, workpaper WP-C04 recorded IG1 Safeguards 4.1–4.7 as Implemented except 4.4, rated Partially implemented because four legacy servers awaited migration. Compliance across 610 managed endpoints stood at 96%, and the company set a target to bring OT engineering laptops under the same baseline by the next review.

WP-C04: use the workpaper format shown in Appendix H.

CHAPTER 11 · CIS CONTROL 5

Account Management

CIS CONTROL 5 · 6 SAFEGUARDS · 4 IN IG1

Account Management

CIS Controls v8.1 · titles quoted verbatim | WP-C05

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 5 — Account Management

Control 5 is about knowing which accounts exist and making sure each one is legitimate, owned, protected by a sound credential and limited to what it is for. It covers three kinds of account: those belonging to people for everyday work, those used for administration, and those used by software, devices and integrations. The six Safeguards build in a natural order. First list every account and check it against reality every quarter (5.1). Make every password unique and long enough (5.2). Remove accounts nobody is using (5.3). Keep administrative power in separate accounts (5.4). Give service accounts their own inventory and review, because they are the most often forgotten (5.5). Finally run all of this from a central directory or identity service so that changes happen once and everywhere (5.6). Control 5 manages the accounts themselves; Control 6 manages what those accounts may reach and how they authenticate.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 11-1. Safeguards of CIS Control 5, Account Management

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
5.1	**“Establish and Maintain an Inventory of Accounts”**	Users	Identify	IG1	Keep one current list of every account the enterprise manages, covering at least ordinary user accounts, administrator accounts and service accounts, recording for each the person or owner, the user-name, the start and end dates and the department. At least every quarter, confirm that each active ac-count is still authorised.
5.2	**“Use Unique Passwords”**	Users	Protect	IG1	Every account on every enterprise asset uses its own password that is not reused elsewhere, including built-in and local administrator accounts. As a work-ing minimum, passwords are at least 8 characters where MFA protects the account and at least 14 characters where it does not.
5.3	**“Disable Dormant Accounts”**	Users	Protect	IG1	Accounts that have not been used for 45 days are disabled or deleted automatically or through a rou-tine check, wherever the system allows it. This re-moves lingering logins belonging to leavers, com-pleted projects and forgotten tests.
5.4	**“Restrict Administrator Privileges to Dedicated Administrator Accounts”**	Users	Protect	IG1	Administrative rights are held only in separate ac-counts used solely for administration. Everyday work such as email, browsing and office documents is done from the person's normal account without ele-vated rights.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
5.5	**“Establish and Maintain an Inventory of Service Accounts”**	Users	Identify	IG2	Keep a separate inventory of non-human accounts used by applications, scripts, scheduled jobs, integrations and devices, recording at least the owning department, the purpose and the date of last review. Review it at least every quarter to confirm each active service account is still authorised.
5.6	**“Centralize Account Management”**	Users	Govern	IG2	Accounts are created, changed and removed through a central directory or identity service rather than separately in each system, so that one action reaches everything the person uses. Systems that cannot connect are listed and managed as exceptions.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
5.1	**1.** Extract accounts from every system that holds its own user store (directory, email tenant, ERP, core business applications, cloud consoles, network devices, key SaaS) into a single register or identity governance tool. **2.** Join the register to the HR record (or contractor register) so each human account carries name, employee or contractor ID, department, start date and end date; flag any account with no match. **3.** Run a quarterly validation: owners or managers confirm each active account, unmatched or unconfirmed accounts are disabled, and the result is signed off and retained.	• Account inventory with the minimum fields populated • Quarterly validation records with sign-off and actions taken • Reconciliation of accounts to HR and contractor lists
5.2	**1.** Set length rules in the directory, applications and devices: a minimum of 8 characters for MFA-protected accounts and 14 for accounts without MFA; prefer passphrases and avoid forced complexity rules that push users to predictable patterns. **2.** Screen new passwords against lists of known breached and common passwords, and deploy a local administrator password solution so each machine's local admin secret is unique and rotated. **3.** Provide an enterprise password manager so staff can hold unique credentials for the many systems that do not support single sign-on.	• Password policy settings from the directory and key applications • Local administrator password management configuration and coverage • Breached-password screening configuration or report
5.3	**1.** Report last successful sign-in per account from the directory and from each application with its own user store. **2.** Disable accounts with no sign-in for 45 days through automation or a weekly scheduled job, with a short, documented exception list (for example statutory or break-glass accounts) owned and reviewed. **3.** Delete disabled accounts after a defined retention period, keeping audit records as required.	• Inactivity report showing last sign-in dates • Automation rule or job record and output • Exception list with owner and review date

Safeguard	Practical steps	Evidence
5.4	1. Issue each administrator a separate named privileged account and remove administrative group membership from their normal account. 2. Remove local administrator rights from users' everyday accounts on endpoints and provide a controlled elevation process for exceptions. 3. Block privileged accounts from email and internet browsing through mailbox policy, conditional access, proxy rules or privileged access workstations.	• Membership of privileged groups mapped to dedicated admin accounts • Endpoint local administrator group report • Policy preventing mail and browsing from admin accounts
5.5	1. Discover service accounts from the directory, databases, cloud identity services (including API keys and workload identities) and application configuration files. 2. Record owner department, named technical owner, purpose, systems used, privilege level, credential type, rotation date and review date for each. 3. Run a quarterly review in which owners confirm need and privilege; disable unclaimed accounts after notice and move secrets into a vault or managed identity.	• Service account inventory with owner, purpose and review date • Quarterly service account review records • Vault or managed identity coverage report
5.6	1. Choose the authoritative directory or identity provider and connect applications through federation, SCIM or connectors. 2. Drive joiner, mover and leaver events from HR into the directory so that accounts follow the employment record. 3. Keep a register of systems with local user stores that cannot be centralised and apply compensating manual reconciliation to them.	• List of applications integrated with the central directory and those not integrated • HR-to-directory integration design and sample event logs

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
IG1 covers four Safeguards: 5.1 (account inventory with quarterly validation), 5.2 (unique passwords of adequate length), 5.3 (disable accounts dormant for 45 days) and 5.4 (administrator rights only in dedicated admin accounts). A 40-person firm can meet these using the admin console of its productivity suite and a spreadsheet: export the user list each quarter, have the partners or office manager tick each name against the staff list, turn on the suite's inactivity report, give the IT person a separate admin login, and switch on a local administrator password tool or set unique local passwords on each laptop.	IG2 adds 5.5 (a separate, quarterly reviewed inventory of service accounts) and 5.6 (central account management through a directory or identity service). These reflect environments with many applications, integrations and scripts, where manual per-system account management breaks down and non-human accounts outnumber people.	No IG3-only Safeguards; IG3 enterprises apply IG1 and IG2 with more rigour, typically through an identity governance tool that automates inventory, certification campaigns and dormant-account action, short-lived or vaulted credentials for service accounts, and privileged access management.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 5.1 → 5.16 Identity management; 5.18 Access rights
- 5.2 → 5.17 Authentication information; 8.5 Secure authentication
- 5.3 → 5.16 Identity management; 5.18 Access rights
- 5.4 → 8.2 Privileged access rights; 5.15 Access control
- 5.5 → 5.16 Identity management; 8.2 Privileged access rights; 5.17 Authentication information
- 5.6 → 5.16 Identity management; 5.15 Access control; 8.5 Secure authentication
- Clause 9.1 (monitoring and measurement) supports the quarterly validation cycle as a measured activity

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: PR.AA-01 (identities and credentials for authorised users, services and hardware are managed) for 5.1–5.3, 5.5, 5.6; PR.AA-05 (access permissions managed with least privilege) for 5.4 (Srida IT mapping)
- NIST SP 800-53 Rev. 5: AC-2 account management, IA-2 and IA-5 identification and authenticator management, AC-6 least privilege
- NIST SP 800-63B for password length and breached-password screening guidance

F India Regulatory Touchpoints

- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6: reasonable security safeguards for personal data, including measures to control access to it; an account inventory and dormant-account rule are common evidence. Mapping is not compliance
- RBI cyber security and IT governance directions for banks and NBFCs: periodic user access review, privileged account control and prompt removal of leavers
- SEBI CSCRF (2024): identity and access management expectations including periodic review of user and privileged accounts for regulated entities
- CERT-In Directions of 28 April 2022: incident reporting within 6 hours and log retention for 180 days depend on being able to attribute activity to accounts

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Most intrusions today do not break in; they log in. Credentials are stolen through phishing, bought from infostealer logs, guessed through password spraying, or reused from a breach of an unrelated website. Once an attacker holds a valid account, their activity looks like ordinary work. Weak spots are predictable: accounts of staff who left months ago, contractor accounts with no end date, test logins created during a project, shared generic IDs, local administrator passwords that are identical on every laptop, and service accounts whose passwords have not changed since the application was installed.

Privileged accounts magnify the damage. An administrator who reads email with a domain admin account turns a single phishing click into control of the whole directory. Service accounts are frequently over-privileged, excluded from MFA and unknown to the security team, which makes them a favourite route for ransomware operators and for persistence after an initial breach. Without an inventory, a review cycle and a dormant-account rule, none of this is visible until an incident.

In India, rapid hiring, heavy use of contract staff and outsourced service desks, and the coexistence of a modern SaaS stack with legacy on-premises applications produce many unsynchronised user stores. Regulators look for this in inspections: RBI and SEBI frameworks expect periodic user access review and prompt removal of leavers, and the DPDP Rules 2025 expect access to personal data to be controlled as part of reasonable security safeguards. A complete, reviewed account inventory is also what allows an enterprise to answer quickly when CERT-In or a regulator asks who had access during an incident.

I Applicability

Applies to every enterprise, since every enterprise has accounts. Small firms usually have few systems but share logins freely; for them the priorities are a named account per person, a quarterly check of the user list against the staff list, and a separate admin login for whoever looks after IT. SaaS-heavy enterprises should treat the identity provider as the core of the inventory but must still find accounts created directly inside SaaS applications, and non-human identities such as API keys and OAuth applications. Enterprises with OT will find shared operator logins on HMIs and vendor accounts on engineering workstations; where these cannot be made individual, record them as exceptions with physical or procedural controls and a named owner. Where an MSP administers systems, its engineers' accounts must appear in the inventory with an end date tied to the contract, and the MSP should not use shared administrator IDs.

J Implementation Guidance

1. Identify every system that holds accounts, starting from the software inventory (Control 2), and decide which will be connected to the central directory or identity provider (5.6) and which will remain local.
2. Build the account inventory (5.1) by extracting accounts from each system and matching them to HR and contractor records; investigate every unmatched account.
3. Separate and tag account types: user, administrator, service, shared or generic, external and emergency (break-glass).

4. Set password rules (5.2) in the directory and applications, deploy breached-password screening, a local administrator password solution and an enterprise password manager.
5. Issue dedicated administrator accounts (5.4), remove admin rights from everyday accounts and block mail and browsing from privileged accounts.
6. Discover and inventory service accounts (5.5), assign owners, reduce privileges and move credentials into a vault or managed identities.
7. Automate dormant-account handling (5.3) at 45 days with a controlled exception list.
8. Connect HR events to the directory so joiners, movers and leavers flow automatically, and connect applications through federation and provisioning (5.6).
9. Run the quarterly validation of user and service accounts, record outcomes and track remediation to closure.
0. Report metrics to management and feed findings into Control 6 access reviews.

K Tools and Automation

- Central directory or identity provider for authoritative account creation, change and removal
- Identity governance and administration (IGA) tools, or simple scripted exports, for account inventory, reconciliation to HR and certification campaigns
- Local administrator password management to give each endpoint a unique, rotated local admin secret
- Enterprise password manager for unique credentials on systems without single sign-on
- Privileged access management or secrets vault for administrator and service account credentials
- Breached-password screening integrated with the directory
- SIEM or directory reporting to monitor new privileged accounts and sign-ins from dormant accounts

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
CISO	Owns the account management standard, approves exceptions and reports metrics
Identity and access management team or IT administrator	Maintains the directory, inventory, automation and dormant-account rule
HR	Provides timely, accurate joiner, mover and leaver data as the authoritative source
Line managers and application owners	Confirm accounts in quarterly validation and request removal of unneeded accounts
Service account owners	Justify each service account, its privilege and credential handling in quarterly reviews
Internal audit or assessor	Tests inventory completeness and operation of reviews and dormant-account handling

M Documentation and Records

- Account management standard covering account types, naming, ownership, passwords and dormancy
- Account inventory and service account inventory
- Quarterly account and service account validation records
- Dormant-account automation design and exception list
- Privileged account standard and list of dedicated admin accounts
- Register of systems not integrated with the central directory
- HR-to-directory integration design

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 11-2. Assessment testing procedures, Control 5

Test ID	Method	Testing procedure	Result

Test ID	Method	Testing procedure	Result
TP-C05-01	EXAMINE	5.1: Examine the account management standard and the account inventory. Confirm that the inventory covers user, administrator and service accounts across all systems with their own user stores, and records at least the person's name, username, start and end dates and department. Identify systems in the software inventory that are not in the account inventory.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-02	RE-PERFORM	5.1: Obtain an independent extract of active accounts from the directory and two or more critical applications, and re-perform the reconciliation to the HR and contractor records at a date of your choosing. Identify accounts with no matching current worker, missing fields, or end dates in the past, and compare with the inventory.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-03	INSPECT	5.1: Inspect the account validation records for each quarter in the review period. Confirm a validation took place at least quarterly, was signed off by the accountable person, and that accounts found unauthorised were disabled with evidence of action.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-04	INSPECT	5.2: Inspect password settings in the directory, the email tenant and a sample of applications and network devices. Confirm minimum length of at least 8 characters where MFA applies and at least 14 characters where it does not, and that breached or common passwords are screened where supported.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-05	SAMPLE	5.2: For a sample of endpoints and servers, confirm the local administrator credential is unique per machine (through the local administrator password management tool or inspection of rotation records). Confirm that shared or default passwords are not used for network devices and appliances in the sample.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-06	RE-PERFORM	5.3: Re-perform a last sign-in analysis on the directory and each in-scope application with its own user store. Identify enabled accounts with no successful sign-in for more than 45 days and confirm each is either disabled, covered by an approved exception, or recently created. Inspect the automation rule or scheduled job and its run history over the period.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-07	EXAMINE	5.3: Examine the dormant-account exception list. Confirm each exception has an owner, justification and review date, and that the list is short and reviewed at least quarterly.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-08	INSPECT	5.4: Inspect membership of privileged groups and roles in the directory, cloud tenants and key applications. Confirm every member is a dedicated administrator account, not a person's everyday account, and that each admin account maps to a named person.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-09	RE-PERFORM	5.4: Using a sample of administrator accounts, re-perform or inspect attempts to use them for email and internet browsing and confirm these are blocked or not provisioned. Inspect the local administrators group on a sample of endpoints and confirm everyday user accounts are not members.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-10	EXAMINE	5.5: Examine the service account inventory. Confirm it records department owner, purpose and review date for each account, and compare it with service accounts discovered in the directory, databases and cloud identity services to test completeness.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-11	SAMPLE	5.5: For each quarter in the period, inspect the service account review. Select a sample of service accounts and confirm the owner confirmed the need and privilege, that unneeded accounts were disabled, and whether credentials are vaulted or rotated.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C05-12	**EXAMINE**	5.6: Examine the identity architecture and the register of applications. Confirm a central directory or identity service is the authoritative source, determine the proportion of in-scope applications integrated with it, and confirm non-integrated systems are recorded with compensating reconciliation.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-13	**SAMPLE**	5.6: Select a sample of leavers and movers from HR records over the period and trace each through the directory and connected applications, confirming that the change was driven from the central service and reached connected systems.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C05-14	**INTERVIEW**	5.1: Interview the IAM administrator, HR and two line managers about how account validation is performed, what happens to unconfirmed accounts and how contractor end dates are captured. Corroborate with the validation records.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Use the review period in the engagement letter, normally twelve months, which gives four quarterly validations for 5.1 and 5.5. Account inventories and dormancy are best tested by whole-population data analysis rather than sampling: extract every enabled account from the directory and from each critical application and compare with HR and last sign-in data. Where manual follow-up is required, sample 25 unmatched or dormant accounts (or all if fewer). For privileged accounts analyse the full population of privileged group members. For local administrator uniqueness sample 10–25 endpoints and 5–10 servers. For service accounts test 100% of the inventory against discovery output and sample 10–15 for review evidence. For centralisation, sample 15–25 leavers and movers across the period, weighting towards involuntary leavers and staff with privileged access. Record the source and extraction date of every population, and extend testing when an exception is found.

P Interview Questions

Interviewee	Question
IAM administrator	Which systems still have their own user lists, and how do you know you have found all of them?
HR manager	How quickly does IT learn of a resignation or termination, and how are contractor end dates recorded?
Line manager	When you last confirmed your team's accounts, what did you actually check, and did you reject any?
System administrator	Show me which account you use to read email and which you use to administer servers.
Application owner	Which service accounts does your application use, what can they do, and when was their password last changed?

Q Technical and Process Verification

- The inventory includes accounts from all systems with local user stores, not only the directory
- Every enabled human account maps to a current worker and every service account to an owner and purpose
- Quarterly validations occurred on time and led to action
- No enabled account is dormant beyond 45 days without an approved exception
- Administrator rights are held only by dedicated accounts and everyday accounts lack local admin
- Password length and uniqueness rules are configured as stated

R Expected Evidence

- Account and service account inventories
- Directory and application account extracts with last sign-in dates
- HR joiner, mover and leaver lists for the period
- Quarterly validation and service account review records
- Password policy configuration screenshots or exports

- Local administrator password management coverage report
- Privileged group membership reports
- Dormant-account automation configuration and run logs
- Register of applications integrated and not integrated with the directory

S Evaluation Criteria

Implemented

- A complete inventory exists and quarterly validations are evidenced with action taken
- Whole-population analysis finds no unauthorised or dormant enabled accounts beyond approved exceptions
- Admin rights are confined to dedicated accounts and passwords meet the length and uniqueness rules

Partially implemented

- The inventory covers the directory but misses applications with their own user stores
- Validations happen but not every quarter, or findings are not acted on
- Dormant accounts are disabled in the directory but not in local systems

Not implemented

- No account inventory or validation exists
- Leavers' accounts remain enabled widely, or administrators use everyday accounts with domain admin rights
- Shared or identical passwords are common across systems

T Common Gaps and Findings

- Condition: 23 enabled accounts in the loan management system belong to people who left more than 60 days ago. Criteria: 5.1 requires quarterly validation that active accounts are authorised; 5.3 requires dormant accounts to be disabled after 45 days. Effect: Former staff or anyone holding their credentials can still reach customer financial data.
- Condition: The local administrator password is identical on all 420 laptops. Criteria: 5.2 requires unique passwords for all enterprise assets. Effect: A single compromised laptop gives an attacker administrative access to every other laptop.
- Condition: Five of seven IT staff use their everyday mailbox account as a domain administrator. Criteria: 5.4 requires dedicated administrator accounts. Effect: A phishing email opened by any of them could compromise the whole directory.
- Condition: No service account inventory exists; discovery found 87 service accounts, 31 with no identifiable owner. Criteria: 5.5 requires an inventory with owner, purpose and review date, reviewed quarterly. Effect: Over-privileged, non-expiring credentials are available to attackers and nobody would notice their misuse.
- Condition: Only the quarter ending June was validated; other quarters have no record. Criteria: 5.1 requires validation at least quarterly. Effect: Unauthorised accounts can persist for up to a year.
- Condition: Six business applications maintain local user lists with no link to the directory. Criteria: 5.6 requires central account management. Effect: Leaver removal depends on manual e-mails and is incomplete.

U Remediation Guidance

- Disable all enabled accounts not matching a current worker immediately, then automate dormancy at 45 days across the directory and connected applications.
- Deploy a local administrator password management solution so every endpoint has a unique, rotated local admin password.
- Issue dedicated admin accounts, remove privileged rights from everyday accounts and block mail and browsing from admin accounts.
- Build the service account inventory, assign owners, remove unclaimed accounts after notice and vault the remaining credentials.
- Calendar the quarterly validation with named reviewers, a deadline and escalation to the CISO for late returns.
- Connect the remaining applications to the identity provider by federation or provisioning, prioritising those holding personal or financial data.

V Monitoring Metrics

- Number of enabled accounts with no matching current worker (target zero)
- Percentage of quarterly validations completed on time (target 100%)
- Number of enabled accounts dormant more than 45 days without exception (target zero)
- Percentage of service accounts with owner, purpose and review date recorded (target 100%)
- Percentage of in-scope applications integrated with the central identity service

W Related Controls and Maturity Indicators

- Control 6 (access granting, revocation, MFA and role-based access)
- 4.7 (default accounts)
- Control 8 (audit logs for account activity)
- Control 2 (software inventory to find user stores)
- Control 14 (awareness of password and credential handling)
- Control 15 (service provider accounts)

Initial	Defined	Managed	Optimised
Accounts are created on request in each system; nobody can produce a full list, leavers are removed when remembered and administrators use their normal accounts.	An inventory, password standard, dormant-account rule and dedicated admin accounts are documented and largely in place; validation happens but relies on manual effort.	Accounts flow from HR through a central directory, quarterly user and service account validations are on time with tracked actions, and dormancy is automated.	Identity governance automates inventory, certification and dormancy across all systems, service accounts use vaulted or short-lived credentials, and metrics drive continuous improvement.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

Fictional scenario — a 600-employee Pune NBFC. The NBFC lends to small traders through 40 branches in Maharashtra and Karnataka. Staff use a directory for Windows sign-in and email, but the loan origination system, the collections application and the vendor-hosted gold-loan module each keep their own user lists. An internal audit before an RBI inspection found that nobody could say how many accounts existed. A Srida IT review extracted 2,140 enabled accounts across the four systems for 612 staff and 85 contractors. It found 214 accounts with no current worker, 96 dormant for over 45 days, a single local administrator password shared by every branch PC, and eight IT staff using their mail accounts as domain admins. Thirty-four service accounts ran integrations between the loan and collections systems; most had passwords set at installation four years earlier.

The NBFC disabled unmatched accounts within a week, deployed a local administrator password tool, issued dedicated admin accounts and created a service account register with owners from IT and Collections. It connected the loan and collections systems to the identity provider through federation and SCIM; the vendor-hosted module was recorded as a non-integrated system with a monthly user list reconciliation sent by the vendor. HR events now create and disable directory accounts automatically. A 45-day dormancy job runs weekly.

Six months later the follow-up assessment, recorded in workpaper WP-C05 (see Appendix H for a completed sample), rated 5.1–5.4 Implemented, 5.5 Partially implemented because two quarterly service account reviews were late, and 5.6 Implemented with the vendor module as a documented exception.

WP-C05: use the workpaper format shown in Appendix H.

CHAPTER 12 · CIS CONTROL 6

Access Control Management

CIS CONTROL 6 · 8 SAFEGUARDS · 5 IN IG1

Access Control Management

CIS Controls v8.1 · titles quoted verbatim | WP-C06

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 6 — Access Control Management

Control 6 governs what accounts are allowed to do and how strongly people must prove who they are before they do it. Control 5 makes sure the right accounts exist; Control 6 decides their access across their whole life. It sets up the two processes at either end of that life, granting access on joining or moving (6.1) and taking it away on leaving or moving (6.2). It requires multi-factor authentication for the three highest-risk situations: applications reachable from the internet (6.3), remote access into the network (6.4) and administration (6.5). For larger enterprises it adds an inventory of the systems that perform authentication and authorisation (6.6) and central enforcement through a directory or single sign-on (6.7). The most mature enterprises define access by role and review it at least annually (6.8). The guiding principle throughout is least privilege: each account gets only the access its role requires, for only as long as it is needed.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 12-1. Safeguards of CIS Control 6, Access Control Management

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
6.1	**“Establish an Access Granting Process”**	Documentation	Govern	IG1	A written process, automated where practical, is followed whenever someone joins or changes role, so that access to enterprise assets is requested, approved by the right person and granted only as far as the role needs. Grants are recorded so they can be traced later.
6.2	**“Establish an Access Revoking Process”**	Documentation	Govern	IG1	A process, automated where practical, removes access promptly when someone leaves, loses a right or changes role, normally by disabling accounts at once rather than deleting them so that audit trails survive. The process reaches every system, including those outside the central directory.
6.3	**“Require MFA for Externally-Exposed Applications”**	Users	Protect	IG1	Every enterprise or third-party application that can be reached from the internet requires multi-factor authentication where the application supports it. Enforcing MFA once at the single sign-on or directory layer is an acceptable way to achieve this.
6.4	**“Require MFA for Remote Network Access”**	Users	Protect	IG1	All remote access into the enterprise network, such as VPN, remote desktop gateways, virtual desktops and zero-trust access brokers, requires multi-factor authentication. This includes access by vendors and support providers.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
6.5	**“Require MFA for Administrative Access”**	Users	Protect	IG1	Every account used for administration requires multi-factor authentication where supported, on all enterprise assets, whether the administration is done by in-house staff on-site or by a service provider. This covers directory, server, network, cloud console, database and SaaS administration.
6.6	**“Establish and Maintain an Inventory of Authentication and Authorization Systems”**	Software	Identify	IG2	Keep a list of the systems that authenticate users or decide what they may do, whether run in-house or by a provider: directories, identity providers, MFA services, PAM, certificate authorities, RADIUS, application-level authentication and authorisation stores. Review and update it at least annually.
6.7	**“Centralize Access Control”**	Users	Protect	IG2	Access to enterprise assets is decided and enforced through a central directory or single sign-on service wherever the assets support it, so that policy, MFA and revocation apply consistently. Systems that cannot be connected are known and handled as exceptions.
6.8	**“Define and Maintain Role-Based Access Control”**	Users	Govern	IG3	Define the access each role in the enterprise needs to do its job, document it, and assign access through those roles. At least once a year, review access to enterprise assets to confirm every privilege is still authorised, and act on what the review finds.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
6.1	**1.** Define who may request and who must approve access for each system (usually the line manager plus the system or data owner for sensitive access). **2.** Drive new-joiner access from HR start events and role templates so standard access is granted automatically, with additional access requested through a ticket or self-service workflow. **3.** On a role change, require a review that removes access no longer needed before new access is granted, to prevent accumulation.	• Access granting procedure • Sample of access requests with approvals matching the access granted • Provisioning workflow or automation configuration
6.2	**1.** Set target timings: same-day or immediate disablement for leavers, immediate for involuntary exits, and removal of old-role access within a set number of days of a move. **2.** Trigger disablement from HR leaver events in the directory, and cascade to connected applications through federation and de-provisioning connectors. **3.** Maintain a checklist for systems with local accounts, physical tokens and remote access, and record completion for each leaver.	• Access revocation procedure with timings • Leaver list reconciled to disablement timestamps • Completed leaver checklists for non-integrated systems

Safeguard	Practical steps	Evidence
6.3	1. List externally reachable applications: email and collaboration suites, SaaS, customer and partner portals that staff administer, web applications published by the enterprise and vendor support portals. 2. Federate them to the identity provider and enforce MFA through conditional access; enable native MFA where federation is not available. 3. Remove legacy authentication protocols that bypass MFA and document applications that cannot support MFA with compensating controls.	• Register of externally exposed applications with MFA status • Conditional access or MFA policy configuration • Sign-in logs showing MFA challenges and absence of legacy authentication
6.4	1. Identify every remote access path, including vendor-installed remote support tools and OT remote maintenance connections. 2. Integrate VPN and remote gateways with the identity provider or an MFA server and refuse connections without a second factor. 3. Close unmanaged remote access paths and make vendor access time-bound and approved per session.	• VPN and remote gateway authentication configuration • Remote access path inventory • Connection logs showing MFA for sampled sessions
6.5	1. List administrative interfaces and privileged accounts from the Control 5 inventory. 2. Enforce MFA through the identity provider, a PAM jump host or native features; prefer phishing-resistant factors such as hardware security keys for the most powerful roles. 3. Require MSPs to use individual accounts with MFA under the enterprise's control, not shared provider credentials.	• MFA status for every privileged account • PAM or jump host configuration • MSP contract clause and evidence of MSP account MFA
6.6	1. Identify authentication and authorisation systems from the software inventory, architecture diagrams and interviews with application owners. 2. Record for each the owner, hosting model, which applications rely on it, the factors it supports, and how it is protected and monitored. 3. Review the list at least once a year and when a new identity system or major application is introduced.	• Inventory of authentication and authorisation systems • Record of the most recent annual review
6.7	1. Federate applications to the identity provider using standard protocols and enforce access through groups or roles held centrally. 2. Apply conditional access policies (device compliance, location, risk) centrally rather than per application. 3. Track the proportion of applications under central control and plan migration for the rest.	• Application federation register • Central access policy configuration • Exception list of non-integrated systems

Safeguard	Practical steps	Evidence
6.8	1. Work with business owners to build a role catalogue for key systems, mapping job functions to the entitlements they need, and identify combinations that breach separation of duties. 2. Assign access by role, handle exceptions as time-bound additions with approval, and keep the catalogue current as systems change. 3. Run access reviews at least annually (more often for privileged and high-risk access), in which owners certify or revoke each entitlement, and verify revocations were carried out.	• Role catalogue with entitlements and SoD rules • Access review campaign records with decisions and completed revocations

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
IG1 includes five Safeguards: 6.1 (access granting process), 6.2 (access revoking process), 6.3 (MFA on externally exposed applications), 6.4 (MFA for remote network access) and 6.5 (MFA for administrative access). For a 40-person CA firm this means a simple written joiner and leaver checklist kept for each person, MFA switched on for every user of the email and cloud suite and for the accounting SaaS, MFA on the firewall VPN or remote desktop gateway, and MFA on all admin logins including the firm's IT support provider.	IG2 adds 6.6 (inventory of authentication and authorisation systems, reviewed annually) and 6.7 (centralised access control through a directory or SSO). These address enterprises with many applications where access decisions scattered across systems cannot be governed or revoked reliably.	IG3 adds 6.8 (role-based access control with at least annual access review). It suits enterprises with complex job structures, sensitive data or regulatory segregation-of-duties expectations, where ad-hoc grants no longer give assurance that access matches need.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 6.1 → 5.15 Access control; 5.18 Access rights; 5.16 Identity management
- 6.2 → 5.18 Access rights; 6.5 Responsibilities after termination or change of employment; 5.11 Return of assets
- 6.3 → 8.5 Secure authentication; 5.17 Authentication information
- 6.4 → 8.5 Secure authentication; 6.7 Remote working; 8.20 Networks security
- 6.5 → 8.2 Privileged access rights; 8.5 Secure authentication
- 6.6 → 5.9 Inventory of information and other associated assets; 8.5 Secure authentication
- 6.7 → 5.15 Access control; 8.3 Information access restriction
- 6.8 → 5.15 Access control; 5.3 Segregation of duties; 5.18 Access rights; 8.3 Information access restriction
- Clause 9.1 (monitoring and measurement) supports access review as a measured activity

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: PR.AA-05 (access permissions, entitlements and authorisations defined, managed, enforced and reviewed with least privilege and separation of duties) for 6.1, 6.2, 6.7, 6.8; PR.AA-03 (users, services and hardware authenticated) for 6.3–6.5; ID.AM-02 for 6.6 (Srida IT mapping)
- NIST SP 800-53 Rev. 5: AC-2 account management, AC-3 access enforcement, AC-5 separation of duties, AC-6 least privilege, IA-2 identification and authentication (including MFA enhancements), PS-4 and PS-5 personnel termination and transfer

F India Regulatory Touchpoints

- RBI cyber security and IT governance directions for banks and NBFCs: MFA for remote and privileged access, timely revocation and periodic access review
- SEBI CSCRF (2024): MFA and identity and access management expectations for regulated entities, scaled by category
- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6: access control over personal data as part of reasonable security safeguards; mapping is not compliance
- IRDAI information and cyber security guidelines for insurers: access management and MFA expectations

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Stolen passwords are cheap and plentiful, which is why MFA on internet-facing applications, VPNs and administration closes off a large share of real-world intrusions. Credential stuffing against webmail, password spraying against VPN portals, and takeover of cloud admin consoles are routine starting points for business email compromise and ransomware. MFA is not perfect, and attackers now use push-fatigue and adversary-in-the-middle phishing, so the factor type matters for the most powerful accounts.

Access also accumulates. People who change roles keep their old rights, project access is never withdrawn, and leavers' accounts on systems outside the directory remain usable. Each extra entitlement widens the damage when an account is compromised and creates room for fraud by insiders, especially where one person can both initiate and approve a transaction. Weak granting and revoking processes are among the most common findings in Indian regulatory inspections and statutory IT audits.

Indian enterprises face specific pressures: large contract and outsourced workforces, vendor remote support into core systems, and SaaS adoption that outpaces central identity integration. Banking and capital-market regulators expect MFA for remote and privileged access and periodic access review. Under the DPDP Rules 2025, controlling who can access personal data is a named element of reasonable security safeguards, and an access log that attributes activity to individuals is essential for breach investigation and reporting.

I Applicability

Applies to all enterprises. Small firms gain the most from MFA on the email and cloud suite, the VPN or remote desktop gateway and any admin console, all of which are usually free features already licensed; the granting and revoking processes can be a one-page checklist per person. SaaS-heavy enterprises should centre this Control on the identity provider and conditional access, but must check that MFA is not bypassed by legacy protocols, app passwords or local accounts inside SaaS applications. OT environments often contain HMIs and controllers that cannot support MFA; apply MFA at the remote access gateway and jump host into the OT zone, and record device-level exceptions. Where an MSP administers systems or provides remote support, require individual MFA-protected accounts under the enterprise's identity control, session approval for vendor access and immediate revocation at contract end.

J Implementation Guidance

1. Use the Control 5 inventory to list systems, account types and owners; write the access granting (6.1) and revoking (6.2) procedures with approvers and timings.
2. Connect HR events to the directory so joiners get baseline access and leavers are disabled automatically; add a checklist for systems that are not connected.
3. Enable MFA for administrators first (6.5), then remote access (6.4), then all internet-facing applications (6.3), and block legacy authentication.
4. Select stronger, phishing-resistant factors for privileged and high-risk users, and define a secure MFA reset process at the service desk.
5. Build the inventory of authentication and authorisation systems (6.6) and review it annually.
6. Federate applications to the central identity service and move access decisions to central groups and policies (6.7).
7. Develop role definitions with business owners for critical systems, including separation-of-duties rules, and assign access by role (6.8).
8. Run access reviews at least annually, and quarterly for privileged and high-risk systems, verifying that revocations are completed.

9. Monitor and report: time-to-revoke for leavers, MFA coverage and review completion.

K Tools and Automation

- Identity provider and single sign-on with conditional access, to enforce MFA and central access policy
- MFA services supporting authenticator apps and phishing-resistant hardware keys
- Identity governance and administration tools for provisioning workflows, role management and access certification
- Privileged access management for brokered, recorded administrative sessions with MFA
- VPN, virtual desktop or zero-trust network access gateways integrated with the identity provider
- SIEM or identity threat detection to alert on MFA bypass attempts, impossible travel and use of disabled accounts

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
CISO	Owns the access control policy, MFA standard and review programme
IAM team or IT administrator	Operates provisioning, de-provisioning, MFA and central access controls
HR	Provides timely joiner, mover and leaver triggers
Line managers	Request and approve access for their staff and certify it in reviews
System and data owners	Approve sensitive access, define roles and SoD rules, and certify entitlements
Service desk	Performs identity verification before MFA resets and password changes
Internal audit or assessor	Tests the design and operation of access processes and MFA coverage

M Documentation and Records

- Access control policy covering least privilege, approval and review
- Access granting and revoking procedures with timings
- MFA standard defining where MFA is required and acceptable factors
- Register of externally exposed applications and remote access paths
- Inventory of authentication and authorisation systems with annual review record
- Role catalogue and SoD rule set
- Access review records and remediation evidence

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 12-2. Assessment testing procedures, Control 6

Test ID	Method	Testing procedure	Result
TP-C06-01	**EXAMINE**	6.1: Examine the access granting procedure. Confirm it defines requesters and approvers by system sensitivity, covers new joiners and role changes, requires removal of old-role access on a move, and states which parts are automated.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-02	**SAMPLE**	6.1: Select a sample of joiners and movers over the review period. For each, compare access granted in the directory and key applications with the approved request or role template, confirming approval preceded the grant and no extra access was given. For movers, confirm prior-role access was removed.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-03	**EXAMINE**	6.2: Examine the access revoking procedure. Confirm it requires disabling (not only deleting) accounts at termination, defines timings for leavers, involuntary exits and role changes, and covers non-integrated systems, remote access tokens and third-party accounts.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C06-04	RE-PERFORM	6.2: Obtain the HR leaver list for the period and re-perform a comparison with account disablement timestamps in the directory and in sampled non-integrated applications. Identify leavers whose accounts were disabled late, remain enabled, or were used after the leaving date.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-05	INSPECT	6.3: Inspect the register of externally exposed applications and compare it with an external attack-surface view (DNS records, published applications and SaaS in the software inventory). For each application, inspect the identity provider or native configuration to confirm MFA is enforced for all users, and that legacy authentication that bypasses MFA is blocked.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-06	RE-PERFORM	6.3: Re-perform sign-in attempts to a sample of external applications with a test account and confirm a second factor is required. Review sign-in logs over the period for successful sign-ins without MFA and confirm each is explained by an approved exception.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-07	INSPECT	6.4: Inspect the configuration of the VPN, remote desktop gateway, virtual desktop and any remote support tools. Confirm MFA is required for every remote connection, including vendor access, and sample connection logs to confirm MFA was applied.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-08	RE-PERFORM	6.5: Using the privileged account population from Control 5, re-perform an analysis of MFA registration and enforcement for every administrative account across the directory, cloud consoles, network devices, databases and SaaS admin roles, including accounts used by service providers. Identify privileged accounts without MFA and confirm they have approved exceptions.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-09	EXAMINE	6.6: Examine the inventory of authentication and authorisation systems. Confirm it includes on-premises and provider-hosted systems with owner, dependent applications and protection, compare it with the software inventory and architecture for completeness, and confirm a review in the last twelve months.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-10	INSPECT	6.7: Inspect the application federation register and identity provider configuration. Determine the proportion of in-scope applications whose access is enforced centrally, confirm central conditional access policies apply to them, and confirm non-integrated systems are recorded with a plan or compensating control.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-11	EXAMINE	6.8: Examine the role catalogue for in-scope critical systems. Confirm roles are documented with their entitlements, approved by business owners, include separation-of-duties rules and are kept current.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-12	SAMPLE	6.8: Inspect access review campaigns in the period and confirm at least one annual review of enterprise asset access (and more frequent reviews for privileged access where policy requires). For a sample of users, re-perform the review against the role catalogue and confirm revocation decisions were carried out.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C06-13	INTERVIEW	6.5: Interview the service desk lead and IAM administrator about how MFA resets and new factor registrations are verified, and how vendor and MSP administrator access is approved and protected. Corroborate with a sample of reset tickets.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Sampling Guidance

Use the review period in the engagement letter, normally twelve months. Leaver revocation is tested on the whole leaver population by data comparison, with manual follow-up on 25 cases (or all if fewer) for non-integrated systems, weighting towards involuntary exits and privileged users. For joiners and movers, sample 25 across at least three critical systems. MFA for privileged accounts is tested on 100% of the privileged population. MFA for external applications is tested on

every application in the register through configuration, with re-performance on 3–5 applications and log review over the period. For remote access, inspect all gateways and sample 10–25 sessions. For role-based access, select every review campaign in the period and re-perform 10–15 users per campaign. Record populations, sources and extraction dates, and extend the sample when exceptions appear.

P Interview Questions

Interviewee	Question
IAM administrator	How do you know an application that someone in Marketing signed up for is protected by MFA?
HR manager	When a dismissal is decided, how and when is IT told?
Service desk lead	If a caller says they have lost their phone and need their MFA reset, what do you do?
Network engineer	List every way a vendor can reach our systems remotely and show me how MFA applies to each.
Business application owner	Who decides what each role in your application may do, and when did you last remove someone's access after a review?

Q Technical and Process Verification

- Access granted matches approved requests or role templates for sampled joiners and movers
- Leavers' accounts were disabled within target across integrated and non-integrated systems
- MFA is enforced, not merely available, for external applications, remote access and every privileged account
- Legacy authentication and other MFA bypasses are blocked
- The authentication systems inventory and central access control are complete and current
- Access reviews occurred at the required frequency and revocations were carried out

R Expected Evidence

- Access control policy, granting and revoking procedures and MFA standard
- Joiner, mover and leaver lists from HR
- Access request tickets and provisioning logs
- Account disablement timestamps from the directory and applications
- Identity provider conditional access and MFA configuration
- VPN and remote gateway configuration and logs
- Privileged account MFA status report
- Inventory of authentication and authorisation systems
- Role catalogue and access review records

S Evaluation Criteria

Implemented

- Granting and revoking processes are documented, followed and timely in sampled cases
- MFA is enforced on all external applications, remote access and privileged accounts with only approved, compensated exceptions
- For IG2/IG3, access is centrally enforced and role-based reviews are completed and acted on

Partially implemented

- Processes exist but some leavers are revoked late or non-integrated systems are missed
- MFA covers email and VPN but not all SaaS, admin consoles or vendor access
- Reviews are performed but revocations are not verified

Not implemented

- No documented granting or revoking process; access is given on informal request
- MFA is absent from remote access or administrative accounts
- No access reviews have been performed

T Common Gaps and Findings

- Condition: 7 of 25 sampled leavers retained enabled accounts in the collections application for 10–48 days. Criteria: 6.2 requires prompt disablement on termination. Effect: Former staff could access borrower data.
- Condition: The VPN uses username and password only for 40 vendor accounts. Criteria: 6.4 requires MFA for remote network access. Effect: A stolen vendor password gives direct network access.

- Condition: 12 cloud console administrators have MFA registered but not enforced, and legacy protocols are allowed for mail. Criteria: 6.3 and 6.5 require MFA to be enforced. Effect: Credential stuffing could succeed without a second factor.
- Condition: Movers keep their previous access; one branch manager promoted to credit can both sanction and disburse loans. Criteria: 6.1 and 6.8 require role-based access and removal of prior-role rights. Effect: Fraud risk through lack of separation of duties.
- Condition: No inventory of authentication systems; three applications use their own login and a forgotten RADIUS server still authorises Wi-Fi. Criteria: 6.6 requires an inventory reviewed annually. Effect: Weak or unmonitored authentication paths remain.
- Condition: The annual access review for the core system was not performed this year. Criteria: 6.8 requires at least annual review. Effect: Excess and unauthorised privileges may persist.

U Remediation Guidance

- Link HR leaver events to automatic disablement and add a tracked checklist with a 24-hour target for non-integrated applications.
- Enforce MFA on the VPN for all accounts, starting with vendors, and make vendor access session-approved.
- Enforce MFA through conditional access for all administrators, prefer hardware keys for the most powerful roles, and block legacy authentication.
- Introduce mover reviews that remove previous-role access and implement SoD rules in the core system.
- Build and review the authentication systems inventory and retire or integrate stray systems.
- Schedule role-based access reviews with deadlines, escalation and verification of revocations.

V Monitoring Metrics

- Percentage of leavers whose accounts were disabled within the target time (target 100%)
- Percentage of privileged accounts with MFA enforced (target 100%)
- Percentage of externally exposed applications enforcing MFA
- Percentage of in-scope applications under central access control
- Percentage of access review campaigns completed on time, with revocations verified

W Related Controls and Maturity Indicators

- Control 5 (account inventory, dormancy and admin accounts)
- 4.7 (default accounts)
- Control 3 (data access and classification)
- Control 8 (logging of access)
- Control 12 (remote access infrastructure)
- Control 15 (service provider access)
- Control 14 (MFA and phishing awareness)

Initial	Defined	Managed	Optimised
Access is given on informal request, removed irregularly, and MFA is used only where a product enabled it by default.	Granting and revoking procedures and an MFA standard are documented; MFA covers external applications, remote access and administrators.	HR-driven provisioning and deprovisioning, central access control, role definitions for key systems, timely reviews and measured revocation times.	Phishing-resistant MFA for privileged users, risk-based conditional access, automated role-based provisioning and continuous access certification informed by usage.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

Fictional scenario — a Hyderabad hospital chain. The chain runs six hospitals and 30 clinics with 3,200 staff, many on rotating contracts. Clinicians use a hospital information system, a laboratory system and a radiology viewer, each with its own login, plus email and collaboration from a cloud suite. A Srida IT assessment found that MFA was enabled for email but not for the radiology viewer published to referring doctors on the internet, that the equipment vendor's remote support connected through an unprotected remote desktop port, and that leaving nurses' accounts in the laboratory system were disabled on average 19 days after exit. Junior doctors who rotated between hospitals accumulated access to patient records at every site.

The chain enforced MFA on the referring-doctor portal through its identity provider, moved vendor support behind an MFA-protected remote access gateway with per-session approval, and connected HR's exit records to the directory, which now disables accounts on the last working day. The hospital information system and laboratory system were federated for sign-on; the radiology viewer followed in the next quarter. With department heads, the CISO built a role catalogue for clinical, nursing, billing and front-desk staff, with site-based access rules, and the first role-based access review removed 1,140 excess entitlements.

In workpaper WP-C06, 6.1–6.5 were rated Implemented except 6.2, which was Partially implemented because two clinic systems still needed manual removal, and 6.8 was rated Partially implemented pending the annual review cycle.

WP-C06: use the workpaper format shown in Appendix H.

CHAPTER 13 · CIS CONTROL 7

Continuous Vulnerability Management

CIS CONTROL 7 · 7 SAFEGUARDS · 4 IN IG1

Continuous Vulnerability Management

CIS Controls v8.1 · titles quoted verbatim | WP-C07

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 7 — Continuous Vulnerability Management

Control 7 is about knowing, continuously, which known weaknesses exist in the enterprise's systems and closing them before an attacker uses them. It joins three activities that are often run separately: watching for new vulnerability information, testing the estate for weaknesses, and applying fixes. The Control asks for a documented process for each half of the cycle (finding and fixing), automated operating system and application patching, regular internal and external scanning, and evidence that findings are actually closed. It depends on Controls 1 and 2: a scanner cannot test an asset nobody knows about, and a patch tool cannot update software that is not inventoried.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 13-1. Safeguards of CIS Control 7, Continuous Vulnerability Management

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
7.1	**“Establish and Maintain a Vulnerability Management Process”**	Documentation	Govern	IG1	The enterprise writes down how it finds, rates, assigns and tracks weaknesses in its hardware, software and cloud services, names who owns each step, and revisits the document at least once a year or whenever the estate or threat picture shifts materially.
7.2	**“Establish and Maintain a Remediation Process”**	Documentation	Govern	IG1	Alongside the discovery process sits a written, risk-based plan for fixing what is found: how severity and business context set the deadline, what happens when a fix cannot be applied, and a review of open items at least monthly.
7.3	**“Perform Automated Operating System Patch Management”**	Software	Protect	IG1	Operating system updates reach servers, laptops, desktops and other managed assets through a tool rather than by hand, on a cycle no slower than monthly, with failures noticed and chased.
7.4	**“Perform Automated Application Patch Management”**	Software	Protect	IG1	Third-party and business applications (browsers, office suites, PDF readers, runtimes, database engines, line-of-business software) are also updated automatically and at least monthly, not only the operating system.
7.5	**“Perform Automated Vulnerability Scans of Internal Enterprise Assets”**	Software	Identify	IG2	Internal assets are scanned for known weaknesses by an automated tool at least every quarter, using both a credentialed scan (logging in to see installed software and settings) and an uncredentialed scan (seeing what an intruder on the network would see).

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
7.6	**“Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets”**	Software	Identify	IG2	Everything the enterprise exposes to the internet, including public IP ranges, websites, VPN gateways, mail servers and cloud-hosted services, is scanned automatically at least monthly from the outside.
7.7	**“Remediate Detected Vulnerabilities”**	Software	Respond	IG2	Weaknesses found by scans, advisories or testing are actually fixed, through tracked work and tooling, following the remediation plan, with progress reviewed at least monthly.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
7.1	**1.** Draft a short vulnerability management procedure covering scope (all asset classes in the Control 1 and Control 2 inventories), intelligence sources, scanning, rating, ticketing, exceptions and reporting. **2.** Name an owner for the procedure and for each step: who subscribes to advisories, who runs scans, who triages, who approves exceptions. **3.** List the advisory feeds the enterprise relies on, for example vendor bulletins, the CERT-In advisories and vulnerability notes, and a known-exploited-vulnerabilities catalogue. **4.** Record a review date and a change trigger (new cloud platform, merger, OT connection, major incident) so the document cannot quietly go stale.	• Approved vulnerability management procedure with version history and last-review date • List of subscribed advisory sources and the named recipient for each • Minutes or sign-off from the most recent annual review
7.2	**1.** Set remediation deadlines by risk tier, combining technical severity (for example CVSS), evidence of active exploitation, exposure (internet-facing or internal) and asset criticality. **2.** Define the exception route: compensating controls, a named risk owner, an expiry date and re-approval when the date passes. **3.** Hold a monthly (or more frequent) remediation review that looks at overdue items, exceptions and trends, and record its decisions. **4.** Align the plan with change management so emergency patching has a fast but still recorded path.	• Remediation procedure with risk tiers and target timelines • Exception register with owners, compensating controls and expiry dates • Minutes or dashboards from the last three monthly remediation reviews
7.3	**1.** Enrol every supported operating system in a patch management or endpoint management tool, including remote laptops that rarely touch the office network. **2.** Use rings: a small pilot group first, then the general population, then critical servers in an agreed window. **3.** Configure reporting so that devices missing updates, or that have not checked in, appear on a weekly exception list. **4.** Treat end-of-support operating systems as a finding under Control 2 and isolate or replace them.	• Patch tool policy configuration showing schedules, rings and deferral limits • Compliance report for a sample month showing per-device patch status • Tickets for devices that failed to patch and their resolution

Safeguard	Practical steps	Evidence
7.4	1. Inventory applications from the Control 2 software list and mark which ones the patch tool can update automatically. 2. Enable automatic updating or packaged deployment for common third-party software; script or schedule the rest. 3. For applications that cannot auto-update (some ERP clients, OT engineering software), record a manual cadence with an owner. 4. Include container base images and libraries in the scope where the enterprise builds its own software, linking to Control 16.	• Application patch catalogue showing which titles are managed automatically • Monthly application patch compliance report • Manual update records for titles outside the automated tool
7.5	1. Define scan scopes from the asset inventory, covering every internal subnet, server segment, cloud VPC/VNet and, carefully, OT zones. 2. Create a least-privilege scan account, protect its credentials in a vault and monitor its use. 3. Schedule credentialed and uncredentialed scans at least quarterly; scan more often for high-risk segments. 4. Reconcile scan results against the inventory so that unscanned or unknown hosts are investigated.	• Scanner schedules and scope definitions • Scan reports for the last four quarters, showing both credentialed and uncredentialed runs • Reconciliation of scanned hosts against the asset inventory
7.6	1. Build and maintain a list of external assets: public IP blocks, DNS names, cloud endpoints and SaaS-hosted portals the enterprise controls. 2. Schedule an external scan at least monthly, and add an ad-hoc scan whenever a new service is published. 3. Compare scan findings with the intended exposure; anything unexpected (an open RDP port, a forgotten test site) is raised as a priority ticket. 4. Where a hosting or cloud provider requires notice before scanning, follow its published rules.	• External asset register • Monthly external scan reports for a sample period • Tickets raised for unexpected exposed services
7.7	1. Feed scan findings automatically, or through a scheduled import, into a ticketing system with owners and due dates set by the remediation tiers. 2. Rescan after each fix to confirm closure rather than trusting the ticket status alone. 3. Report overdue items, ageing and exceptions monthly to IT leadership and quarterly to senior management. 4. Escalate actively exploited vulnerabilities on internet-facing assets for emergency handling.	• Vulnerability tickets with discovery date, due date, closure date and verification scan • Monthly remediation status report • Emergency change records for exploited vulnerabilities

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
An IG1 enterprise documents how it handles vulnerabilities (7.1) and how it decides what to fix and by when (7.2), and it patches operating systems (7.3) and applications (7.4) automatically, at least monthly. For a 40-person firm this usually means turning on the built-in update services of the operating system and browser, managing them through an endpoint or MDM console, subscribing to a handful of vendor and CERT-In advisories, and keeping a one-page procedure with a monthly check of what failed.	IG2 adds active testing and proof of closure: authenticated and unauthenticated internal scans at least quarterly (7.5), external scans at least monthly (7.6), and tracked remediation of what the scans find, reviewed at least monthly (7.7). This is where a scanner, a ticketing workflow and agreed deadlines by severity become necessary.	Control 7 has no IG3-only Safeguards. IG3 enterprises apply all seven Safeguards with more rigour: continuous or agent-based scanning rather than quarterly, risk-based prioritisation using exploitation intelligence, tighter deadlines for internet-facing assets, coverage of OT, containers and cloud configuration, and independent penetration testing under Control 18.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 7.1 → 8.8 Management of technical vulnerabilities; 5.7 Threat intelligence; clause 7.5 Documented information
- 7.2 → 8.8 Management of technical vulnerabilities; clause 6.1.3 Information security risk treatment; 8.32 Change management
- 7.3 → 8.8 Management of technical vulnerabilities; 8.19 Installation of software on operational systems
- 7.4 → 8.8 Management of technical vulnerabilities; 8.19 Installation of software on operational systems
- 7.5 → 8.8 Management of technical vulnerabilities; 8.9 Configuration management
- 7.6 → 8.8 Management of technical vulnerabilities; 8.20 Networks security
- 7.7 → 8.8 Management of technical vulnerabilities; 8.32 Change management; clause 10.2 Nonconformity and corrective action

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: ID.RA-01 (vulnerabilities identified and recorded), ID.RA-02 (threat intelligence), ID.RA-08 (vulnerability disclosure handling), PR.PS-02 (software maintained commensurate with risk), ID.IM-02 (Srida IT mapping, not an official CIS mapping)
- NIST SP 800-53 Rev. 5: RA-5 Vulnerability Monitoring and Scanning; SI-2 Flaw Remediation; SI-5 Security Alerts, Advisories, and Directives; CM-8 System Component Inventory
- CIS publishes official mappings of v8.1 to other frameworks; check them on the CIS website before citing

F India Regulatory Touchpoints

- CERT-In advisories and vulnerability notes: a sensible intelligence input for 7.1; the CERT-In Directions of 28 April 2022 list exploitation of vulnerabilities and attacks on servers and applications among incidents to be reported within six hours.
- SEBI Cybersecurity and Cyber Resilience Framework (CSCRF, 2024): expects regulated entities to run vulnerability assessment and penetration testing at defined intervals and close findings within set timelines, with frequency depending on the entity category.
- RBI directions on IT governance, risk, controls and assurance (2023) and cyber security frameworks for banks and NBFCs: expect patch and vulnerability management, periodic VA/PT and board-level reporting.
- CERT-In empanelled information security auditing organisations: many government and regulated buyers require VA/PT to be performed by an empanelled auditor; confirm the current list on the CERT-In website.

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Most intrusions that do not start with a stolen password start with a known, unpatched flaw. Ransomware crews and access brokers routinely scan the whole internet within days of a vulnerability in a VPN appliance, file-transfer server or web framework becoming public, and they keep exploiting old flaws for years because so many organisations never apply the fix. A weakness nobody has looked for is a weakness nobody is fixing; a scanner report nobody acts on gives a false sense of comfort.

Failure is expensive and visible. An exploited edge device can give an attacker a foothold that bypasses multi-factor authentication altogether, and unpatched internal servers let a single compromised laptop become an enterprise-wide incident. Regulators, insurers and customers increasingly ask not only whether the enterprise scans, but how quickly it closes critical items, and they expect to see numbers.

In India, CERT-In issues advisories and vulnerability notes that many sector regulators expect regulated entities to act on, and the CERT-In Directions of April 2022 make several resulting incidents reportable within six hours. Sector frameworks such as SEBI's CSCRF and RBI's IT governance directions set expectations for periodic vulnerability assessment and penetration testing, often by CERT-In empanelled auditors. For small Indian firms the common failure is simpler: pirated or end-of-life software that cannot be patched at all, which makes Control 2 hygiene a precondition for Control 7.

I Applicability

Every enterprise has vulnerabilities, so Control 7 applies universally; only the shape changes. A small professional firm with laptops and SaaS mostly needs reliable automatic updates and a monthly check that they worked; its external attack surface may be little more than its website and email, which the hosting provider partly covers. A cloud- and SaaS-heavy start-up shifts effort to cloud configuration scanning, container image scanning and dependency checks in its pipelines, while still patching its laptop fleet. Enterprises with OT (factories, hospitals with medical devices) must scan cautiously, often passively, because aggressive scans can disrupt controllers, and many devices cannot be patched on the normal monthly cycle; compensating controls under Controls 12 and 13 then matter. Where IT is outsourced to an MSP, the enterprise remains accountable: the contract should require scanning, patch cadence and monthly reporting, and the enterprise should see the reports, not merely be told the work is done.

J Implementation Guidance

1. Confirm the asset and software inventories (Controls 1 and 2) are good enough to scope scanning and patching; list gaps as the first findings.
2. Write the vulnerability management procedure (7.1) and the remediation procedure with risk tiers and deadlines (7.2); have them approved by the CISO or IT head.
3. Subscribe named people to vendor bulletins, CERT-In advisories and a known-exploited-vulnerabilities feed, and define how an advisory becomes a ticket.
4. Enable automated OS patching (7.3) through endpoint management, with pilot and production rings and a defined maintenance window for servers.
5. Extend automation to third-party applications (7.4); record manual cadences for anything that cannot be automated.
6. Deploy a vulnerability scanner; configure quarterly credentialed and uncredentialed internal scans (7.5) and monthly external scans (7.6).
7. Integrate findings with ticketing, assign owners, and verify closure by rescanning (7.7).
8. Stand up a monthly remediation review with an exception register; report ageing and overdue critical items to senior management quarterly.
9. Over time, move towards continuous agent-based assessment and prioritisation using exploitation data, and schedule independent penetration tests under Control 18.

K Tools and Automation

- Endpoint or unified endpoint management (UEM/MDM): schedules and enforces OS and application updates, reports device patch state, including for remote laptops.
- Third-party patch catalogue or packaging tool: keeps common applications (browsers, runtimes, PDF readers) current where the OS update service does not.
- Network vulnerability scanner (for example OpenVAS/Greenbone, or commercial equivalents): performs credentialed and uncredentialed scans of internal and external assets.
- Agent-based vulnerability assessment or EDR with vulnerability module: gives near-continuous visibility for laptops that are seldom on the corporate network.
- Cloud security posture management and container image scanning: find misconfigurations and vulnerable packages in cloud workloads and pipelines.
- Ticketing or IT service management system: tracks findings to closure with owners, due dates and exceptions.
- CIS Benchmarks and CIS-CAT style assessment tools as configuration references; confirm current availability and licensing.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
CISO / Head of Information Security	Owns the vulnerability and remediation procedures, approves risk tiers and exceptions, reports to senior management.
IT Operations / Infrastructure Lead	Runs patch automation for servers and endpoints, maintains maintenance windows and rings.

Role	Responsibility
Vulnerability Management Analyst (may be part-time in SMEs)	Runs scans, triages findings, raises tickets, verifies closure, maintains the external asset list.
Application and System Owners	Fix or accept findings on their systems within the agreed deadlines, test patches, request exceptions.
Change Advisory Board / Change Manager	Approves routine and emergency patch changes and keeps records.
MSP or Hosting Provider (where used)	Delivers contracted patching and scanning and supplies reports and evidence.

M Documentation and Records

- Vulnerability management procedure (scope, sources, scanning, roles, review cycle)
- Remediation procedure with risk tiers, target timelines and exception handling
- Patch management standard covering rings, windows, deferral limits and end-of-support handling
- Scan schedules and scope definitions, including the external asset register
- Vulnerability exception (risk acceptance) register
- Monthly remediation review minutes and management reports

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 13-2. Assessment testing procedures, Control 7

Test ID	Method	Testing procedure	Result
TP-C07-01	**EXAMINE**	7.1: Examine the vulnerability management procedure. Confirm it covers all asset classes, names advisory sources and owners, defines scanning and triage, and has been reviewed within the last 12 months or after the last significant change.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-02	**INTERVIEW**	7.1: Interview the person responsible for advisory monitoring. Ask them to show how the last critical advisory (for example a CERT-In note or vendor emergency bulletin) was received, assessed against the inventory and turned into a ticket.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-03	**EXAMINE**	7.2: Examine the remediation procedure. Confirm deadlines are set by risk (severity, exploitation, exposure, criticality), that an exception route with expiry exists, and that a review at least monthly is required.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-04	**SAMPLE**	7.2: Select the last three months of remediation review records and a sample of five open exceptions. Confirm each review occurred, decisions were recorded, and each exception has an owner, compensating control and unexpired approval.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-05	**INSPECT**	7.3: Inspect the patch management console. Confirm OS update policies are automated, scheduled at least monthly, and cover servers, desktops and remote laptops; note any devices excluded and why.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-06	**SAMPLE**	7.3: Select 25 assets across asset types and locations from the inventory. For each, compare the installed OS patch level with the latest vendor release over the last three monthly cycles; record any asset more than one cycle behind without an approved exception.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-07	**SAMPLE**	7.4: For the same sample, check the versions of three commonly installed applications (for example browser, office suite, PDF reader) against current vendor releases. Confirm updates are applied automatically and at least monthly, or under a documented manual cadence.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C07-08	**EXAMINE**	7.5: Examine internal scan schedules and reports for the last four quarters. Confirm both credentialed and uncredentialed scans ran each quarter, credentialed scans actually authenticated (check authentication success rates), and coverage matched the inventory.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-09	**RE-PERFORM**	7.5: Take a list of hosts from one scanned subnet in the scanner and compare it to the asset inventory and DHCP records for the same subnet. Investigate any host in one list but not the other.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-10	**EXAMINE**	7.6: Examine the external asset register and monthly external scan reports for a six-month period. Confirm every month has a scan, every listed external asset was in scope, and unexpected exposed services were ticketed.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-11	**RE-PERFORM**	7.6: Using the enterprise's public DNS records and IP allocations, identify internet-facing hosts independently (with permission) and compare them to the external asset register.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-12	**SAMPLE**	7.7: Select 20 vulnerabilities rated critical or high from scans in the last six months. For each, trace discovery date, ticket, due date per the remediation tier, closure date and verification rescan; record any overdue item without an exception.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C07-13	**OBSERVE**	7.7: Observe a monthly remediation review meeting (or examine its recording or minutes). Confirm overdue items, ageing and exceptions are discussed and actions are assigned.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Draw samples from the Control 1 asset inventory, not from the patch tool, so that unmanaged assets have a chance of being selected. For endpoints and servers, a sample of 25 across sites, operating systems and business units is usually enough for a mid-sized enterprise; for an IG1 firm under 50 devices, examine every device. Test patching over at least three monthly cycles and scanning over at least two quarters (internal) or six months (external) so that the result reflects operation rather than a one-off effort before the assessment. For remediation, sample findings by severity, weighting critical and internet-facing items, and include a few items closed early in the period to confirm rescans actually happened.

P Interview Questions

Interviewee	Question
CISO	How do you decide which vulnerabilities are fixed first, and what deadlines apply to critical findings on internet-facing systems?
IT Operations Lead	Which devices or applications are not covered by automated patching, and how are they kept current?
Vulnerability Analyst	How do you know your credentialed scans are authenticating successfully, and what do you do with hosts that the scanner finds but the inventory does not list?
Application Owner	Describe the last time you could not apply a patch on time. What compensating control was used and who approved the exception?
MSP Account Manager	What patch and scan reports do you send the enterprise each month, and how are failures escalated?

Q Technical and Process Verification

- Patch tool coverage matches the asset inventory within an agreed tolerance, and excluded devices are justified.
- Sampled assets are within one monthly cycle of current OS and application updates, or have approved exceptions.
- Internal scans run at least quarterly in both credentialed and uncredentialed modes; external scans at least monthly.
- Critical and high findings are closed within the remediation tier deadlines and closure is confirmed by rescanning.
- Exceptions are time-bound, owned and backed by compensating controls.

R Expected Evidence

- Approved vulnerability management and remediation procedures with review history
- Advisory subscription list and an example advisory-to-ticket trail
- Patch tool configuration and three months of compliance reports
- Internal scan reports for the last four quarters showing authentication success
- External asset register and six months of external scan reports
- Vulnerability tickets with due dates, closure dates and rescan evidence
- Exception register
- Monthly remediation review minutes and quarterly management reports

S Evaluation Criteria

Implemented

- Documented procedures for discovery and remediation exist, are approved and have been reviewed in the last year.
- OS and application patching is automated and sampled assets are current within one monthly cycle.
- Scans run at the required frequency (IG2+) with credentialed coverage, and critical findings are closed within deadline and verified.
- Monthly remediation reviews happen and exceptions are controlled.

Partially implemented

- OS patching is automated but third-party applications are updated ad hoc or not at all.
- Scanning occurs but credentialed scans fail to authenticate on a significant share of hosts, or external scans are irregular.
- Findings are ticketed but closure is not verified and overdue items are not escalated.

Not implemented

- No documented process; patching depends on individual users or administrators.
- No vulnerability scanning at IG2 or above, or scan results are not acted on.
- Large numbers of end-of-support systems remain in production without isolation or plan.

T Common Gaps and Findings

- Condition: Remote laptops have not checked in to the patch tool for over 60 days. Criteria: 7.3 requires automated OS updates at least monthly across enterprise assets. Effect: The most exposed devices, used on home and public networks, run with known exploitable flaws.
- Condition: Only OS updates are automated; browsers, runtimes and PDF readers are months behind. Criteria: 7.4 requires automated application updates at least monthly. Effect: Phishing and drive-by attacks targeting common applications succeed despite a patched OS.
- Condition: Credentialed internal scans authenticate on fewer than half of the Windows servers. Criteria: 7.5 requires both authenticated and unauthenticated scans. Effect: Scan reports understate risk; missing patches and weak settings stay invisible.
- Condition: A VPN gateway with a publicly exploited vulnerability remained unpatched for seven weeks. Criteria: 7.2 and 7.7 require risk-based deadlines and monthly remediation. Effect: High likelihood of external compromise bypassing MFA, and a probable CERT-In reportable incident.
- Condition: The external asset list omits a marketing microsite hosted by an agency. Criteria: 7.6 requires scanning of all externally exposed assets. Effect: An unmanaged, outdated site carries the enterprise's brand and could be defaced or used for credential theft.
- Condition: Exceptions have no expiry and some date back three years. Criteria: 7.2 requires a maintained, risk-based remediation process. Effect: Temporary risk acceptance has become permanent without anyone re-deciding.

U Remediation Guidance

- Enforce a check-in policy for endpoints, using cloud-based management so remote devices patch without VPN, and quarantine devices that do not report for 30 days.
- Add a third-party application catalogue to the patch tool and set auto-update for browsers and common runtimes.
- Fix scan credentials (correct accounts, firewall rules for remote management) and track authentication success as a scan quality metric.
- Introduce an emergency patch path with 72-hour or shorter targets for actively exploited internet-facing vulnerabilities, approved by the CISO.

- Rebuild the external asset register from DNS, IP allocations, cloud accounts and agency contracts, and add discovery scanning to find new exposures.
- Give every exception an expiry of at most 12 months, require re-approval, and report expiring exceptions in the monthly review.

V Monitoring Metrics

- Percentage of managed assets fully patched for OS and in-scope applications within 30 days of vendor release (target at least 95 percent).
- Median and 90th percentile days to remediate critical and high findings, split into internet-facing and internal.
- Credentialed scan authentication success rate (target at least 95 percent of in-scope hosts).
- Number of open critical findings past deadline without an approved exception (target zero).
- Percentage of inventory assets scanned in the last quarter (internal) and month (external).

W Related Controls and Maturity Indicators

- Control 1 (asset inventory sets scan and patch scope)
- Control 2 (software inventory; removing unsupported software)
- Control 4 (secure configuration; misconfigurations found by scans)
- Control 10 (malware defences as compensating control)
- Control 12 and 13 (segmentation and monitoring where patching is not possible)
- Control 16 (application software security and dependency management)
- Control 18 (penetration testing validates vulnerability management)

Initial	Defined	Managed	Optimised
Updates are left to users or applied when someone remembers; there is no scanning and no record of what is missing.	Procedures for discovery and remediation are written; OS and major applications auto-update; scans run on a schedule but follow-up is uneven.	Patching and scanning cover the full inventory, deadlines are tracked with metrics, closure is verified by rescans, and exceptions are controlled and reported monthly.	Assessment is near-continuous, prioritisation uses exploitation intelligence and business context, remediation is largely automated, and trends feed investment and architecture decisions.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A 600-employee Pune NBFC ran monthly Windows updates and an annual VA/PT by an external auditor and considered Control 7 covered. A readiness review against the CIS Controls found three problems. First, the patch console listed 540 devices, while the HR-linked asset register showed 610; most of the gap was field-collection laptops that connected only over mobile data and never reached the on-premises update server. Second, the browser and PDF reader on sampled devices were up to five versions old because only Microsoft updates were automated. Third, the annual test reports contained the same medium and high findings in two consecutive years, with no tickets behind them. The CISO wrote a two-page remediation procedure: actively exploited internet-facing flaws within three days, other critical findings within 15 days, highs within 30 days, and a monthly review chaired by the CTO. Endpoint management moved to a cloud-based service so laptops patched over any connection, and third-party applications were added to the catalogue. A scanner was deployed internally, with credentialed scans monthly for servers and quarterly for the wider estate, and monthly external scans of the lending portal and VPN. Within four months, devices current within 30 days rose from 71 to 96 percent, credentialed authentication reached 97 percent, and repeat findings disappeared from the next VA/PT. The NBFC also mapped its remediation evidence to its RBI IT governance obligations so that the same reports served the board, the auditor and the regulator.

WP-C07: use the workpaper format shown in Appendix H.

CHAPTER 14 · CIS CONTROL 8

Audit Log Management

CIS CONTROL 8 · 12 SAFEGUARDS · 3 IN IG1

Audit Log Management

CIS Controls v8.1 · titles quoted verbatim WP-C08

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 8 — Audit Log Management

Control 8 is about producing a reliable record of what happens on the enterprise's systems and actually using it. It covers deciding what to log, switching logging on, keeping enough storage, aligning clocks, capturing richer detail where sensitive data lives, collecting specific high-value records (DNS queries, web requests, command lines), bringing logs together, keeping them long enough, reviewing them regularly, and extending all of this to service providers. Logs serve two purposes: detecting an attack while it is in progress, and reconstructing what happened afterwards for containment, regulators, insurers and courts. Without the second, an enterprise often cannot say whether data was taken, and must assume the worst.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 14-1. Safeguards of CIS Control 8, Audit Log Management

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
8.1	**“Establish and Maintain an Audit Log Management Process”**	Documentation	Govern	IG1	The enterprise has a written logging standard that says which assets and events must be logged, where logs go, who looks at them and how often, how long they are kept and how they are protected, and it revisits that standard at least annually or after a significant change.
8.2	**“Collect Audit Logs”**	Data	Detect	IG1	Logging is switched on, as the standard requires, across the enterprise's assets; default settings that log little or nothing are not left in place.
8.3	**“Ensure Adequate Audit Log Storage”**	Data	Protect	IG1	Wherever logs are written, locally or centrally, there is enough space to hold them for the period the standard requires, and someone is warned before space runs out and logs are overwritten or dropped.
8.4	**“Standardize Time Synchronization”**	Data	Protect	IG2	All assets that support it take their time from the same approved sources, with at least two synchronised sources configured, so that timestamps from different systems can be lined up during an investigation.
8.5	**“Collect Detailed Audit Logs”**	Data	Detect	IG2	Systems that hold or process sensitive data log in enough detail to reconstruct what happened: which source, when, which account, from where to where, and what was done, so that a forensic investigator can follow the trail.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
8.6	**“Collect DNS Query Audit Logs”**	Data	Detect	IG2	DNS lookups made by enterprise assets are logged where this is practical and supported, so that contact with malicious or suspicious domains can be detected and investigated.
8.7	**“Collect URL Request Audit Logs”**	Data	Detect	IG2	Requests to web addresses made from enterprise assets are logged where practical and supported, so that downloads, phishing clicks and command-and-control traffic over the web can be traced.
8.8	**“Collect Command-Line Audit Logs”**	Data	Detect	IG2	Commands typed or scripted on servers and workstations, especially through shells and remote administration tools, are captured, because attackers rely heavily on built-in command-line tools once inside.
8.9	**“Centralize Audit Logs”**	Data	Detect	IG2	Logs from across the estate are brought together in one place, as far as is practical, under the logging standard, so that events from different systems can be searched, correlated and kept consistently.
8.10	**“Retain Audit Logs”**	Data	Protect	IG2	Audit logs are kept for at least 90 days across enterprise assets; Indian entities should treat the CERT-In 180-day rolling period as their practical floor, and longer where a sector rule requires.
8.11	**“Conduct Audit Log Reviews”**	Data	Detect	IG2	People or automated analytics look at logs at least weekly to spot unusual or suspicious activity, and the reviews are recorded and followed up.
8.12	**“Collect Service Provider Logs”**	Data	Detect	IG3	Where the provider makes them available, the enterprise collects logs from its cloud, SaaS and other service providers, such as sign-ins and permission decisions, data creation and deletion, and user administration.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
8.1	**1.** Draft a logging standard organised by asset tier (identity systems, servers holding sensitive data, network edge, endpoints, cloud and SaaS, OT) with the minimum events for each tier. **2.** Set collection, review and retention requirements, reconciling CIS's 90-day minimum with stricter Indian obligations such as the CERT-In 180-day rolling retention and any sector rule. **3.** Assign owners: who configures sources, who runs the log platform, who reviews, who answers regulator or CERT-In requests for logs. **4.** Record a review date and change triggers (new cloud tenant, new regulator direction, SIEM migration, major incident).	• Approved audit log management standard with version history • Log source matrix mapping asset tiers to required events, destinations and retention • Record of the most recent annual review

Safeguard	Practical steps	Evidence
8.2	**1.** Enable operating system audit policies through group policy, configuration management or MDM baselines (Control 4) so logging survives rebuilds. **2.** Turn on logging in network devices, firewalls, VPNs, identity providers, databases, key applications and cloud control planes. **3.** Maintain a source inventory linked to the asset inventory and flag assets that should log but do not. **4.** Alert when a source that normally sends logs falls silent.	• Audit policy baselines (GPO, MDM or configuration management exports) • Log source inventory reconciled with the asset inventory • Silent-source alert configuration and examples
8.3	**1.** Size local event logs so that they will not roll over before collection, and configure the behaviour when full (overwrite only after forwarding). **2.** Capacity-plan the central platform from daily ingest volume times retention period, with headroom for incident spikes. **3.** Monitor storage utilisation and ingestion licence limits and alert at agreed thresholds. **4.** Include log storage in backup and archive planning so that older logs move to cheaper storage rather than being deleted early.	• Local log size settings in baselines • Capacity plan and current storage utilisation for the log platform • Storage threshold alert configuration and recent alerts
8.4	**1.** Run at least two internal NTP servers (or use two approved upstream sources) and point every asset at them through baselines. **2.** For Indian entities, synchronise upstream to the NTP services of NIC or NPL, or to sources traceable to them, as the CERT-In Directions require; document the specific servers used. **3.** Use a consistent time zone or UTC in logs and record the convention in the logging standard. **4.** Monitor clock drift and NTP failures, and include cloud and SaaS time sources in the record.	• NTP configuration on internal time servers showing upstream sources • Baseline or sample device configurations showing two time sources • Drift monitoring report or alert configuration
8.5	**1.** Identify sensitive-data assets from the Control 3 data inventory and classify them as the highest logging tier. **2.** Configure verbose logging: successful and failed authentication, privilege use, object and record access, configuration changes, data export, with source and destination addresses. **3.** Enable database and application audit features for access to personal and financial data, not just operating system logs. **4.** Test that a sample event contains every field the standard requires.	• List of sensitive-data assets mapped to the detailed logging tier • Database and application audit configuration • Sample log records showing the required fields
8.6	**1.** Enable query logging on internal resolvers, or use a protective DNS or filtering service (Control 9.2) that keeps per-client query logs. **2.** Make sure logs identify the requesting client (internal IP or device), not only the forwarding resolver. **3.** Forward DNS logs to the central platform and consider volume and retention costs. **4.** Cover roaming devices whose DNS does not pass through office resolvers.	• Resolver or DNS service query logging configuration • Sample DNS query records showing client, query and time • Ingest confirmation in the central log platform

Safeguard	Practical steps	Evidence
8.7	**1.** Enable logging on the web proxy, secure web gateway or firewall URL filtering feature used for Control 9.3. **2.** Ensure records include user or device, full URL or domain, category, action and time. **3.** Decide, with privacy and legal input, how TLS-inspected traffic is logged and who may view it. **4.** Forward URL logs centrally and apply the retention standard.	• Proxy or gateway logging configuration • Sample URL log records • Privacy note or approval covering web activity logging
8.8	**1.** Enable script block and module logging and transcription for PowerShell, and process-creation events with command-line arguments on Windows. **2.** On Linux and Unix, use auditd or equivalent rules for executed commands, and record privileged session activity. **3.** Capture sessions through bastion hosts or PAM for remote administration (SSH, RDP). **4.** Protect these logs from tampering by the administrators whose actions they record.	• Windows audit and PowerShell logging policy settings • Linux audit rules on a sample of servers • PAM or bastion session recording configuration and sample
8.9	**1.** Deploy a central log platform or SIEM (self-hosted, cloud or a managed SOC service). **2.** Onboard sources in priority order: identity, edge, sensitive-data systems, endpoints, cloud and SaaS, then the rest. **3.** Normalise fields and timestamps; tag each source with its owner and asset tier. **4.** Track onboarding coverage against the source inventory and report gaps.	• Central platform architecture and source list • Coverage report: required sources versus sources sending logs • Parsing or normalisation rules for key sources
8.10	**1.** Set retention in the central platform and on any systems that hold their own logs (cloud services, SaaS, appliances) to the longest applicable requirement. **2.** Use tiered storage (hot for searching, archive for retention) and confirm archived logs can be restored and searched. **3.** Protect retained logs against alteration and deletion: write-once storage, restricted delete rights, integrity checks. **4.** Record where logs are stored, including whether they remain within Indian jurisdiction as the CERT-In Directions expect.	• Retention settings on the central platform and key source systems • Oldest available log record for sampled sources • Archive restoration test record
8.11	**1.** Define review use cases: failed and successful logins at odd hours, new administrator accounts, disabled logging, unusual data export, connections to bad domains. **2.** Automate detection rules and dashboards where possible; assign a reviewer and a backup for each weekly review. **3.** Record each review (date, reviewer, items noted, tickets raised), even when nothing is found. **4.** Escalate suspected incidents into the incident response process (Control 17), mindful of CERT-In six-hour reporting.	• Log review procedure and use-case list • Review records for a sample of weeks • Tickets or incidents raised from log reviews

Safeguard	Practical steps	Evidence
8.12	1. List service providers that hold enterprise data or identities and record what logs each can export and at which licence tier. 2. Enable and forward provider audit logs (identity provider, email and collaboration suite, cloud control plane, payroll or CRM SaaS) to the central platform. 3. Write contract clauses requiring log availability, retention and support for investigations, including CERT-In requests. 4. Check periodically that the feeds are still arriving after provider changes.	• Service provider log availability register • Configuration of provider log exports and their ingestion • Contract clauses on log access and retention

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
An IG1 enterprise writes a simple logging standard (8.1), turns on logging across its assets (8.2) and makes sure there is enough space so logs are not lost before they are needed (8.3). For a 40-person Kochi CA firm this may mean enabling the audit logs in its cloud email and identity tenant, enabling Windows security auditing through its device management tool, enlarging local event logs, and recording in one page what is kept where. Indian IG1 firms that are body corporates should note that the CERT-In 180-day rolling retention and NTP synchronisation apply to them regardless of IG, so in practice they must pull forward elements of 8.4 and 8.10.	IG2 adds most of the Control: standard time synchronisation with at least two sources (8.4), detailed logs for sensitive-data systems (8.5), DNS (8.6), URL (8.7) and command-line (8.8) logging, a central log platform (8.9), retention of at least 90 days (8.10) and log review at least weekly (8.11). This is the level at which a SIEM or managed SOC service, or at least a well-run open-source log stack, becomes necessary.	IG3 adds collection of service provider logs where providers support it (8.12): identity, data lifecycle and user administration events from cloud and SaaS platforms. IG3 enterprises also apply the IG2 Safeguards with more rigour: near-real-time correlation, tamper-evident storage, threat hunting over long retention periods, and tested procedures to produce logs quickly for regulators and investigators.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 8.1 → 8.15 Logging; 5.1 Policies for information security; 5.37 Documented operating procedures; clause 7.5 Documented information
- 8.2 → 8.15 Logging; 8.9 Configuration management
- 8.3 → 8.15 Logging; 8.6 Capacity management
- 8.4 → 8.17 Clock synchronization
- 8.5 → 8.15 Logging; 5.28 Collection of evidence; 8.2 Privileged access rights
- 8.6 → 8.15 Logging; 8.16 Monitoring activities
- 8.7 → 8.15 Logging; 8.16 Monitoring activities; 8.23 Web filtering
- 8.8 → 8.15 Logging; 8.2 Privileged access rights; 8.18 Use of privileged utility programs
- 8.9 → 8.15 Logging; 8.16 Monitoring activities
- 8.10 → 8.15 Logging; 5.33 Protection of records; 5.31 Legal, statutory, regulatory and contractual requirements
- 8.11 → 8.16 Monitoring activities; 5.25 Assessment and decision on information security events
- 8.12 → 5.22 Monitoring, review and change management of supplier services; 5.23 Information security for use of cloud services; 8.15 Logging

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: PR.PS-04 (log records generated and made available for continuous monitoring), DE.CM-01, DE.CM-03, DE.CM-06 (external service provider activity monitored), DE.CM-09, DE.AE-02, DE.AE-03 (information correlated from multiple sources), RS.AN-03 (Srida IT mapping, not an official CIS mapping)
- NIST SP 800-53 Rev. 5: AU family (AU-2 Event Logging, AU-3 Content of Audit Records, AU-4 Audit Log Storage Capacity, AU-6 Audit Record Review, AU-8 Time Stamps, AU-9 Protection of Audit Information, AU-11 Audit Record Retention, AU-12 Audit Record Generation); SC-45 System Time Synchronization; SI-4 System Monitoring

- NIST SP 800-92 (Guide to Computer Security Log Management) as background reading; a revision has been in progress
- CIS publishes official mappings of v8.1 to other frameworks; check them on the CIS website before citing

F India Regulatory Touchpoints

- CERT-In Directions of 28 April 2022 under section 70B(6) of the IT Act: enable logs of all ICT systems and maintain them securely for a rolling 180 days within Indian jurisdiction; provide them to CERT-In with an incident report or on direction; report specified incidents within six hours. CERT-In's FAQs on the Directions discuss scope and storage location and should be read alongside them.
- CERT-In Directions on time: connect to the NTP servers of the National Informatics Centre (NIC) or the National Physical Laboratory (NPL), or to NTP servers traceable to them; entities spanning several countries may use another accurate source provided it does not deviate from NIC/NPL time. Commonly cited hosts include samay1.nic.in, samay2.nic.in and time.nplindia.org; confirm current hostnames before configuring.
- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6: reasonable security safeguards for personal data are expected to include logging, monitoring and retention of logs and personal data for a defined period (reported as one year) to detect and investigate unauthorised processing; r.7 sets breach intimation to the Data Protection Board, which relies on log evidence.
- SEBI CSCRF (2024) and RBI cyber security directions: expect centralised logging, SOC monitoring (for some SEBI entity categories through a Market SOC or own SOC) and log retention periods that may exceed 180 days; IRDAI's information and cyber security guidelines also align log retention with CERT-In.

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Attackers rarely announce themselves. They log in with stolen credentials, use the system's own administration tools, and move slowly to avoid notice; the traces they leave are in authentication records, command lines, DNS lookups and web requests. When those records are missing, overwritten after a few days, or scattered across systems with clocks that disagree, intrusions run for months, and investigators cannot establish when they started or what was touched. Attackers know this and frequently clear or disable logs as an early step, so a silent log source is itself a signal.

The cost of weak logging appears after an incident. Without trustworthy logs the enterprise cannot scope a breach, so it may have to notify every customer rather than the affected few, rebuild every system rather than the compromised ones, and accept an insurer's or regulator's assumption of the worst case. Courts and regulators also expect evidence with a sound chain of custody and consistent timestamps.

India has made logging a legal obligation for a very wide set of entities. The CERT-In Directions of 28 April 2022 require service providers, intermediaries, data centres, body corporates and government organisations to enable logs of all ICT systems, keep them securely for a rolling 180 days within Indian jurisdiction, and produce them to CERT-In on request, and they require clocks to be synchronised with NIC or NPL time sources or sources traceable to them. The DPDP Rules 2025 add an expectation of logs and their retention as part of reasonable security safeguards for personal data, and sector regulators such as SEBI under CSCRF set their own retention and SOC monitoring expectations. For an Indian enterprise, CIS's 90-day minimum is therefore a starting point, not the target.

I Applicability

Control 8 applies to every enterprise, and in India the CERT-In Directions make logging a legal duty for most organisations regardless of size. A small firm that is mostly SaaS can meet much of the Control from its cloud email, identity and endpoint management consoles, provided it checks that the licence tier actually retains audit logs for long enough; many entry tiers keep only 30 or 90 days, which falls short of 180. Cloud-heavy start-ups should treat control-plane logs (API calls, IAM changes, storage access) as primary sources and export them to storage they control. OT environments (a Chennai auto-parts plant, for instance) often cannot run agents on controllers; log at the network boundary, from historians and engineering workstations, and from jump hosts instead, and include OT clocks in the time synchronisation scheme because PLC and HMI clocks drift. Where an MSP or managed SOC runs logging, the enterprise should own the retention decision and be able to obtain raw logs within hours, since CERT-In requests go to the enterprise, not the provider.

J Implementation Guidance

1. Map legal and contractual logging obligations (CERT-In, DPDP, sector regulator, customer contracts) and set the retention floor and storage location rules before buying anything.

2. Write the logging standard (8.1) with a source matrix by asset tier, and get it approved by the CISO and, for personal data, the DPO or privacy lead.
3. Fix time first (8.4): build two internal NTP servers synchronised to NIC or NPL sources, push them through baselines, and monitor drift, so every later log line is comparable.
4. Enable logging on all assets through baselines (8.2) and size local storage (8.3), starting with identity providers, domain controllers, firewalls, VPNs and cloud tenants.
5. Stand up a central log platform or managed SOC service (8.9) and onboard sources in priority order, tracking coverage against the source inventory.
6. Add the high-value detailed sources: verbose logs on sensitive-data systems (8.5), DNS queries (8.6), URL requests (8.7) and command lines (8.8).
7. Set retention (8.10) to the longest applicable requirement, use tiered and tamper-resistant storage, and test that archived logs can be restored and searched.
8. Start weekly reviews (8.11) using a short list of use cases and automated rules; record every review and connect escalation to incident response.
9. Extend collection to service providers (8.12), upgrading licence tiers where needed and adding log access clauses to contracts.
0. Rehearse a CERT-In log request: produce 180 days of logs for a named system within an agreed time, and fix whatever slows it down.

K Tools and Automation

- SIEM or central log management platform (self-hosted, cloud-native or delivered through a managed SOC): collects, normalises, correlates, retains and alerts on logs from all sources.
- Open-source log stacks and host agents, for example Wazuh, or syslog collectors feeding a search platform: an affordable route for SMEs if someone owns tuning and upkeep.
- Endpoint telemetry tools (EDR, osquery, Sysmon-style process logging, Velociraptor for collection during investigations): capture process, command-line and network activity.
- Privileged access management and bastion hosts: record administrative sessions and commands for 8.8.
- Protective DNS resolvers and secure web gateways: generate per-client DNS and URL logs for 8.6 and 8.7 while also filtering (Control 9).
- NTP servers (internal stratum servers, optionally with a GNSS reference) and drift monitoring for 8.4.
- Write-once or object-lock storage and hashing tools to protect retained logs against tampering.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
CISO / Head of Information Security	Owns the logging standard, sets retention with legal input, approves use cases and reports on coverage and review.
SOC Lead or Log Platform Owner	Runs the central platform, onboarding, parsing, storage capacity and detection rules.
System, Network and Cloud Administrators	Enable and maintain logging and time synchronisation on their platforms; must not be able to alter their own audit trail.
Log Reviewers / SOC Analysts	Perform and record weekly (or continuous) reviews and escalate suspected incidents.
DPO / Privacy Lead and Legal Counsel	Advise on lawful monitoring of employees, retention of personal data in logs and regulatory production requests.
Incident Response Lead	Uses logs for investigation, coordinates CERT-In reporting and log production.
Vendor / Service Provider Manager	Ensures provider contracts include log availability, retention and investigation support.

M Documentation and Records

- Audit log management standard, including the source matrix, retention schedule and storage location rules

- Log source inventory linked to the asset inventory
- Time synchronisation standard naming internal NTP servers and their upstream NIC/NPL sources
- Log platform architecture, capacity plan and onboarding tracker
- Log review procedure, use-case catalogue and review records
- Log protection and access procedure (who can read, export or delete logs)
- Procedure for producing logs to CERT-In, regulators or law enforcement
- Service provider log availability register and contract clauses

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 14-2. Assessment testing procedures, Control 8

Test ID	Method	Testing procedure	Result
TP-C08-01	EXAMINE	8.1: Examine the audit log management standard. Confirm it defines events by asset tier, collection, review frequency, retention period, storage location and protection, and that it was reviewed within the last 12 months or after the last significant change. Check that the retention period reflects the CERT-In 180-day requirement and any sector rule.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-02	INTERVIEW	8.1: Interview the CISO and legal or privacy lead. Ask how the retention period and storage location were decided and who answers a CERT-In request for logs.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-03	INSPECT	8.2: Inspect the audit policy baselines (GPO, MDM profiles, configuration management) and confirm they enable the events required by the standard.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-04	SAMPLE	8.2: Select 25 assets from the asset inventory across types (servers, endpoints, network devices, cloud services). For each, confirm logging is enabled as the standard requires and that a log from the last 24 hours exists locally or centrally.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-05	INSPECT	8.3: Inspect local log size settings on sampled assets and storage utilisation on the central platform. Confirm local logs do not roll over before collection, capacity alerts exist, and no storage-full or dropped-event conditions occurred in the last 90 days.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-06	INSPECT	8.4: Inspect the configuration of the internal NTP servers. Confirm at least two time sources are configured, upstream sources are NIC/NPL or traceable to them, and the servers report synchronised status.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-07	RE-PERFORM	8.4: For ten sampled assets including a domain controller, a firewall, a Linux server, a cloud VM and (if present) an OT device, query the current time and NTP status and compare to the reference. Record any drift beyond the tolerance in the standard.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-08	SAMPLE	8.5: From the list of sensitive-data systems, select five. Retrieve sample log records for a login, a privileged action and a data access or export. Confirm each record shows source, date and time, user, source and destination address and the action.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-09	EXAMINE	8.6: Examine DNS resolver or protective DNS logging configuration and sample records. Confirm queries are attributable to individual clients and are forwarded to the central platform, including for roaming devices.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-10	EXAMINE	8.7: Examine proxy, gateway or firewall URL logging and sample records. Confirm user or device, URL or domain, action and time are captured, and that a privacy approval covers the logging.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C08-11	RE-PERFORM	8.8: With permission, run a harmless test command (for example a PowerShell command listing local users, and a sudo command on a Linux server) and confirm the command line appears in the central platform within the expected time, with account and host.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-12	EXAMINE	8.9: Examine the central platform's source list and compare it with the log source inventory. Calculate coverage of required sources and list required sources not sending logs.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-13	OBSERVE	8.9: Observe an analyst search for one user's activity across identity, endpoint and network sources for a given hour. Confirm the results can be correlated with consistent timestamps.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-14	RE-PERFORM	8.10: For five sampled sources, retrieve the oldest available record. Confirm retention meets at least 90 days and the enterprise's own requirement (for Indian entities, normally 180 days rolling), including for SaaS and cloud services that hold their own logs.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-15	INSPECT	8.10: Inspect protection of retained logs: who holds delete or modify rights, whether write-once or integrity controls are used, where storage is located, and the result of the last archive restoration test.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-16	SAMPLE	8.11: Select eight weeks from the last six months. For each, obtain the record of log review showing reviewer, date, use cases covered and follow-up. Confirm reviews occurred at least weekly and that findings led to tickets or incidents.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-17	INTERVIEW	8.11: Interview a reviewer. Ask them to describe the last suspicious item they found and how it was escalated, and what they do when a source stops sending logs.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C08-18	EXAMINE	8.12: Examine the service provider log register and the ingestion of provider logs for the identity provider, email and collaboration suite, and main cloud platform. Confirm authentication, data creation and deletion, and user administration events are collected where the provider supports them, and that contracts address log access.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Draw asset samples from the asset inventory, not from the SIEM's source list, so that assets that never send logs can be detected. A sample of 25 assets across types and sites suits a mid-sized enterprise; IG1 firms should check every critical system (identity tenant, email, file storage, firewall) rather than sample. For time synchronisation include at least one of each platform type, since drift usually affects network appliances, OT devices and virtual machines restored from snapshots. For retention, test the oldest record rather than the configured setting, because licence limits, storage purges and misconfigured indexes often delete data earlier than the policy says. For reviews, sample weeks across the whole period, including holiday weeks, because that is when reviews tend to lapse.

P Interview Questions

Interviewee	Question
CISO	What retention period does the enterprise apply to logs, where are they stored, and how quickly could you hand CERT-In 180 days of logs for a named server?
SOC Lead	How do you find out that a log source has stopped sending, and how long did the last such gap last before it was noticed?
Network Administrator	Which time sources do firewalls, switches and the VPN use, and how do you know they are in sync?
Cloud Administrator	Which cloud and SaaS audit logs are exported to the central platform, and what licence tier is required for each to retain logs long enough?

Interviewee	Question
DPO / Privacy Lead	How are employees informed about web, DNS and command-line logging, and who may view these logs?
System Administrator	Can you, or another administrator, delete or edit the audit records of your own actions? Show me.

Q Technical and Process Verification

- The logging standard covers collection, review, retention and protection and reflects Indian legal requirements.
- Sampled assets have logging enabled and logs reach the central platform; silent sources are detected.
- All sampled assets synchronise to at least two approved time sources with drift within tolerance.
- Detailed, DNS, URL and command-line logs exist for in-scope assets and contain the required fields.
- The oldest retrievable logs meet the retention requirement, and logs are protected from tampering.
- Weekly reviews are recorded and lead to action; provider logs are collected where supported (IG3).

R Expected Evidence

- Approved audit log management standard and source matrix
- Audit policy baselines and sampled device configurations
- NTP server configurations and drift check results
- Central platform source list and coverage report
- Sample log records for detailed, DNS, URL and command-line logging
- Retention settings and oldest-record evidence for sampled sources
- Log protection settings and archive restoration test
- Weekly review records and resulting tickets
- Service provider log register and contract clauses

S Evaluation Criteria

Implemented

- A current logging standard exists, logging is enabled on sampled assets and storage is adequate (IG1).
- Clocks are synchronised to two approved sources; detailed, DNS, URL and command-line logs are centralised and retained at least 90 days, and at least 180 days for Indian entities subject to CERT-In.
- Weekly reviews are recorded and acted on; logs are protected against tampering.
- Service provider logs are collected where supported (IG3).

Partially implemented

- Logging is enabled but local logs overwrite before collection, or important source types are missing from the central platform.
- Retention is configured at 90 days, meeting CIS but not the CERT-In 180-day requirement.
- Reviews happen but are irregular, unrecorded or limited to alerts without periodic look-back.

Not implemented

- No logging standard; default logging settings with no central collection.
- Clocks are not synchronised, making correlation across systems unreliable.
- No one reviews logs; they are consulted only after an incident, if at all.

T Common Gaps and Findings

- Condition: The cloud email and identity tenant runs on a licence tier that keeps sign-in and audit logs for 30 days. Criteria: 8.10 requires at least 90 days; the CERT-In Directions require 180 days rolling. Effect: Investigation of a mailbox compromise discovered after two months has no records, and the enterprise cannot meet a CERT-In production request.
- Condition: Firewalls and switches use their factory default time sources and drift by up to seven minutes. Criteria: 8.4 requires standard synchronisation with at least two sources; CERT-In requires NIC/NPL-traceable time. Effect: Network events cannot be aligned with endpoint and identity events, weakening timelines and evidential value.
- Condition: PowerShell script block logging and process command-line capture are disabled. Criteria: 8.8 requires command-line audit logs. Effect: Hands-on-keyboard attacker activity using built-in tools leaves almost no trace.

- Condition: Domain administrators hold delete rights on the SIEM index. Criteria: 8.1 and 8.10 require logs to be protected under the logging process. Effect: An attacker with stolen admin credentials, or a malicious insider, can erase evidence.
- Condition: Weekly log review is assigned to one engineer and no records exist for 11 of the last 26 weeks. Criteria: 8.11 requires reviews at least weekly. Effect: Suspicious activity can go unnoticed for weeks, increasing dwell time and the chance of missing the six-hour CERT-In reporting window.
- Condition: Logs from the payroll SaaS provider are not collected and the contract is silent on log access. Criteria: 8.12 requires service provider logs where supported. Effect: Unauthorised changes to bank details for salary credit cannot be traced.

U Remediation Guidance

- Upgrade the identity and email licence tier, or export audit logs daily to enterprise-controlled storage with 180-day or longer retention, and document the decision.
- Deploy two internal NTP servers synchronised to NIC or NPL sources, push them to all devices through baselines, and alert on drift above one second for servers and five seconds for other devices.
- Enable PowerShell script block, module and transcription logging and process creation auditing with command lines through group policy; add auditd rules on Linux.
- Separate log platform administration from domain administration, enable object lock or write-once storage, and alert on any deletion attempt.
- Assign a reviewer and a backup, automate the core use cases, and record each weekly review in a ticket even when no issue is found.
- Add a log access and retention clause to the payroll SaaS contract and onboard its audit export into the SIEM.

V Monitoring Metrics

- Percentage of required log sources sending to the central platform (target at least 95 percent).
- Median time to detect a silent log source (target under 24 hours).
- Percentage of sampled assets within clock drift tolerance (target 100 percent of servers and network devices).
- Retention achieved for each critical source, measured by the oldest retrievable record (target at least 180 days for Indian entities).
- Percentage of weeks with a recorded log review in the last quarter (target 100 percent), and number of incidents first detected through log review.

W Related Controls and Maturity Indicators

- Control 1 and 2 (inventories define log sources)
- Control 3 (data inventory identifies sensitive-data systems for 8.5)
- Control 4 (baselines enforce audit policies and NTP settings)
- Control 5 and 6 (account and access events are key log content)
- Control 9 (DNS and URL filtering generate 8.6 and 8.7 logs)
- Control 13 (network monitoring and alerting build on centralised logs)
- Control 15 (service provider management supports 8.12)
- Control 17 (incident response depends on log evidence)

Initial	Defined	Managed	Optimised
Logging is left at vendor defaults, logs stay on each device and are overwritten within days; clocks are unmanaged and nobody reviews anything.	A logging standard exists, key sources are enabled and partly centralised, retention is set, and NTP is configured, but coverage gaps and irregular reviews remain.	Required sources are centralised and monitored for silence, clocks are synchronised to approved sources, retention meets CIS and Indian requirements and is verified, logs are tamper-protected, and reviews are recorded weekly with metrics.	Detection is continuous and tuned from incidents and threat intelligence, threat hunting uses long retention, provider logs are fully integrated, and log production for regulators is rehearsed and fast.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A Hyderabad hospital chain with eight sites, a hospital information system, a laboratory system, cloud email and around 2,500 endpoints discovered, after a ransomware attempt was stopped by its EDR, that it could not tell how the attacker got in. Domain controller logs had rolled over after four days, the firewall clock was 11 minutes fast, the cloud email tenant kept sign-in logs for 30 days, and nobody had ever looked at the HIS audit trail. The incident still had to be reported to CERT-In within six hours, and the hospital could provide little supporting evidence. The CISO rebuilt Control 8 over six months. A one-page logging standard set 180 days of searchable retention and one year of archive for systems holding patient data, reflecting the CERT-In Directions and the DPDP Rules. Two internal NTP servers were built at the data centre, synchronised to NIC and NPL sources, and pushed to all servers, network devices and, through the biomedical engineering team, to the modality workstations. Logging baselines turned on detailed Windows auditing, PowerShell logging and Linux auditd, and HIS and laboratory database auditing was enabled for access to patient records. Instead of buying a large SIEM, the hospital engaged a managed SOC under a contract that kept raw logs in an Indian region, gave the hospital direct read access and required weekly review reports. The email tenant licence was upgraded so that audit data was retained and exported. At the next quarterly test, the security team produced 180 days of logs for a named HIS server in under two hours, and an analyst traced a test user's activity across firewall, endpoint and HIS records within a single consistent timeline.

WP-C08: use the workpaper format shown in Appendix H.

CHAPTER 15 · CIS CONTROL 9

Email and Web Browser Protections

CIS CONTROL 9 · 7 SAFEGUARDS · 2 IN IG1

Email and Web Browser Protections

CIS Controls v8.1 · titles quoted verbatim | WP-C09

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 9 — Email and Web Browser Protections

Control 9 is about the two applications through which most attacks reach people: the web browser and the email client. Users open links and attachments from strangers every day, so these are where phishing, credential-harvesting pages, malicious downloads and fraudulent payment requests land. The Control reduces that exposure in layers: keep browsers and mail clients supported and current, filter dangerous destinations at the DNS and URL level, control extensions, authenticate the enterprise's own mail domains with SPF, DKIM and DMARC, strip risky attachment types, and scan what remains for malware. It works alongside awareness training (Control 14) and malware defences (Control 10); technical filtering lowers the number of bad messages and pages that reach users, and training helps with the ones that get through.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 15-1. Safeguards of CIS Control 9, Email and Web Browser Protections

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
9.1	**“Ensure Use of Only Fully Supported Browsers and Email Clients”**	Software	Protect	IG1	Only browsers and email clients that the vendor still supports may run on enterprise assets, and they are kept at the current release the vendor ships; outdated or unsupported versions are blocked or removed.
9.2	**“Use DNS Filtering Services”**	Devices	Protect	IG1	Every end-user device, on the office network or away from it, resolves domain names through a filtering service that refuses lookups for domains known to be malicious.
9.3	**“Maintain and Enforce Network-Based URL Filters”**	Network	Protect	IG2	Web traffic from all enterprise assets passes through network-level filtering that blocks sites which are dangerous or not approved, using categories, reputation scores or block lists that are kept up to date.
9.4	**“Restrict Unnecessary or Unauthorized Browser and Email Client Extensions”**	Software	Protect	IG2	Browser extensions, plug-ins and email client add-ins that are not needed or not authorised are uninstalled or disabled, so that only reviewed additions can run.
9.5	**“Implement DMARC”**	Network	Protect	IG2	The enterprise publishes SPF and DKIM for its mail domains and then a DMARC policy, and checks DMARC on inbound mail, so that others find it harder to send convincing mail pretending to come from the enterprise's domains.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
9.6	**“Block Unnecessary File Types”**	Network	Protect	IG2	The email gateway refuses attachment types the business does not need, such as executables, scripts, disk images and macro-enabled documents, before they reach users.
9.7	**“Deploy and Maintain Email Server Anti-Malware Protections”**	Network	Protect	IG3	Mail servers or gateways run maintained anti-malware protection that inspects attachments and, where appropriate, detonates them in a sandbox before delivery.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
9.1	**1.** Approve a short list of browsers and email clients in the software inventory (Control 2) and record their support status. **2.** Enable automatic updates through the patch or endpoint management tool (Control 7.4) and limit how long users can defer a browser restart. **3.** Use application control or software inventory reports to detect and remove unapproved or end-of-support browsers and mail clients, including portable copies. **4.** Check embedded browser components and legacy compatibility modes that some line-of-business applications depend on.	• Approved browser and email client list with support status • Version report from endpoint management for a sample date • Application control or removal records for unapproved clients
9.2	**1.** Choose a protective DNS approach: a filtering resolver for office networks plus an agent or managed device configuration for roaming laptops and mobiles. **2.** Enforce the setting through MDM or group policy and block outbound DNS to unapproved resolvers at the firewall, including common DNS-over-HTTPS endpoints where feasible. **3.** Enable threat categories (malware, phishing, command-and-control, newly registered domains) and keep a short, reviewed allow-list. **4.** Forward DNS filtering logs to the central platform (links to 8.6).	• DNS filtering service configuration and enabled categories • MDM or policy settings enforcing the resolver on roaming devices • Firewall rules restricting outbound DNS
9.3	**1.** Deploy URL filtering on a secure web gateway, proxy, next-generation firewall or cloud-delivered service, covering office, remote and server traffic. **2.** Define a category policy approved by management (for example block malware, phishing, gambling, anonymisers and uncategorised newly seen sites) and decide on TLS inspection with privacy input. **3.** Keep filtering feeds updated automatically and review override and exception requests on a schedule. **4.** Apply stricter egress policies to servers, which should reach only the sites they need.	• URL filtering policy with approved categories • Gateway configuration showing feed updates and coverage • Exception and override log with approvals

Safeguard	Practical steps	Evidence
9.4	1. Inventory installed extensions and add-ins using browser management policies or endpoint tools. 2. Set a default-deny or allow-list policy through browser and email client management, with a request route for new extensions. 3. Review requested extensions for permissions, publisher and data access before approval. 4. Re-review the allow-list periodically and remove extensions that have changed ownership or permissions.	• Browser and mail client extension management policies • Extension allow-list with approval records • Inventory report of installed extensions
9.5	1. List every domain the enterprise owns, including parked and marketing domains, and every service that sends mail on its behalf. 2. Publish SPF records and enable DKIM signing for each legitimate sending service. 3. Publish DMARC starting at monitoring (p=none) with aggregate reporting, then move to quarantine and reject once legitimate senders align; publish reject records for domains that never send mail. 4. Enable DMARC, SPF and DKIM evaluation on inbound mail at the gateway.	• DNS records (SPF, DKIM, DMARC) for each domain • DMARC aggregate report summaries showing alignment over time • Inbound gateway authentication policy
9.6	1. Identify file types the business genuinely exchanges by email, with input from departments. 2. Configure the gateway to block or quarantine risky types by true file type, not only by extension, including inside archives. 3. Handle password-protected archives by quarantine or release on request after checking. 4. Review the block list and release requests periodically.	• Email gateway attachment policy • Quarantine and block logs for a sample period • Approved exceptions for business-required file types
9.7	1. Enable anti-malware scanning on the mail gateway or cloud mail service, with automatic signature and engine updates. 2. Add sandboxing or detonation for unknown attachments and time-of-click URL checking where available. 3. Define handling of detected items (quarantine, notify, admin release) and retroactive removal of messages later found malicious. 4. Monitor detection volumes and feed alerts to the SOC.	• Mail anti-malware and sandbox configuration • Engine and signature update status • Detection and retroactive removal reports

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
An IG1 enterprise ensures only supported, up-to-date browsers and email clients run (9.1) and uses DNS filtering on all end-user devices, including remote ones (9.2). For a 40-person CA firm this is achievable by managing one approved browser through endpoint management with automatic updates, and pointing devices at a protective DNS service, with an agent or profile for laptops used at clients' offices and at home.	IG2 adds network-based URL filtering for all assets (9.3), control of browser and mail client extensions (9.4), DMARC with SPF and DKIM (9.5) and blocking of unnecessary attachment types at the email gateway (9.6). Many of these are settings in an existing cloud mail service or firewall, so the effort is mostly policy, testing and upkeep rather than new products.	IG3 adds anti-malware protection on the email server or gateway, including attachment scanning and sandboxing (9.7). IG3 enterprises also apply the earlier Safeguards with more rigour: DMARC at reject for all domains, TLS inspection with clear privacy rules, browser isolation for high-risk users, and retroactive removal of malicious messages.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 9.1 → 8.8 Management of technical vulnerabilities; 8.19 Installation of software on operational systems
- 9.2 → 8.23 Web filtering; 8.20 Networks security; 8.7 Protection against malware
- 9.3 → 8.23 Web filtering; 8.20 Networks security
- 9.4 → 8.19 Installation of software on operational systems; 8.9 Configuration management
- 9.5 → 5.14 Information transfer; 8.21 Security of network services
- 9.6 → 8.7 Protection against malware; 5.14 Information transfer
- 9.7 → 8.7 Protection against malware; 8.21 Security of network services

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: PR.PS-02 (software maintained), PR.PS-05 (unauthorised software prevented), PR.IR-01 (networks protected from unauthorised logical access), DE.CM-01 (networks monitored), DE.CM-09 (Srida IT mapping, not an official CIS mapping)
- NIST SP 800-53 Rev. 5: SC-7 Boundary Protection; SI-3 Malicious Code Protection; SI-8 Spam Protection; CM-7 Least Functionality; CM-11 User-Installed Software; SC-20/SC-21 DNS services
- Email authentication standards: SPF (RFC 7208), DKIM (RFC 6376), DMARC (RFC 7489, with an updated DMARC specification in progress at the IETF)
- CIS publishes official mappings of v8.1 to other frameworks; check them on the CIS website before citing

F India Regulatory Touchpoints

- CERT-In Directions of 28 April 2022: phishing attacks, malicious code attacks and compromise of email accounts fall within reportable incident types with a six-hour window, so email and web defences reduce reportable events and their logs support reports.
- CERT-In and NIC guidance on email security: government email policy and CERT-In advisories have recommended SPF, DKIM and DMARC and phishing defences; private entities can treat them as good practice.
- RBI cyber security frameworks for banks and NBFCs and SEBI CSCRF: expect anti-phishing measures, email authentication, web filtering and monitoring of brand-abuse domains.
- DPDP Act 2023 s.8(5): reasonable security safeguards to prevent personal data breaches; phishing-led mailbox compromise is a common breach route, so these controls form part of the safeguards story, and a breach may need intimation under r.7 of the DPDP Rules 2025.

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Phishing remains the most common first step in intrusions and fraud. A single click can install a loader, hand over a password and MFA token through a proxy login page, or start a business email compromise in which an attacker, writing from a lookalike or compromised mailbox, persuades finance staff to change a supplier's bank details. Browser weaknesses and malicious extensions let attackers steal session cookies and read data from web applications without any password at all.

When these defences are missing, the cost tends to be direct money loss and reputational damage rather than only technical clean-up. Spoofed mail from an enterprise's own domain damages customer trust, and without DMARC the enterprise also cannot see who is abusing its name. Unfiltered DNS and web access let malware call home freely and make it harder to contain an infection.

Indian enterprises see heavy volumes of invoice, GST, courier and KYC-themed phishing, and fraud through compromised email is a recurring concern for regulators and the police. CERT-In's Directions list phishing attacks and targeted scanning among reportable incidents with a six-hour window, and CERT-In and sector regulators periodically issue advisories on email security and domain authentication. For SMEs that trade internationally, DMARC alignment increasingly affects whether their invoices reach customers at all, because large mailbox providers have tightened sender requirements.

I Applicability

Control 9 applies to almost every enterprise because almost every enterprise uses email and the web. A small firm on a cloud mail suite will find most Safeguards available as settings: attachment blocking, malware scanning, DMARC evaluation and extension policies, so the job is to switch them on and check them, plus adding a protective DNS service and

managing one browser. Cloud- and SaaS-heavy start-ups rely on the browser as their main work surface, which raises the importance of 9.1 and 9.4 and of browser management in general. OT and server networks should have tight egress rules, with web access only to named update sites, rather than general URL filtering. Where an MSP or hosting provider runs mail and DNS, the enterprise should still own the domains, see the DMARC reports and approve filter policies; DNS records for domains registered by an agency or former employee are a frequent weak point.

J Implementation Guidance

1. Inventory mail domains, sending services, browsers and mail clients in use; agree an approved browser and client list.
2. Enforce supported, auto-updating browsers and clients through endpoint management and remove unapproved ones (9.1).
3. Deploy DNS filtering for office networks and roaming devices, and block outbound DNS to unapproved resolvers (9.2).
4. Turn on network-based URL filtering for users and servers with an approved category policy and exception process (9.3).
5. Move browsers and mail clients to managed extension allow-lists and remove unapproved extensions (9.4).
6. Publish SPF and DKIM, then DMARC at p=none with reporting; analyse reports, fix legitimate senders and progress to quarantine and reject; add reject records for non-sending domains (9.5).
7. Configure the mail gateway to block unneeded file types by true type, including inside archives (9.6).
8. Enable mail anti-malware with sandboxing and time-of-click URL checks, and integrate detections with the SOC (9.7).
9. Connect DNS, URL and mail logs to the central platform (Control 8) and run periodic phishing simulations under Control 14 to measure what still gets through.

K Tools and Automation

- Browser and email client management policies (via endpoint management or MDM): enforce versions, updates, safe settings and extension allow-lists.
- Protective DNS service or filtering resolver, with endpoint agents for roaming devices: blocks known malicious domains and logs queries.
- Secure web gateway, proxy, next-generation firewall URL filtering or cloud-delivered web security: category and reputation filtering, optional TLS inspection.
- Email security gateway or the security features of the cloud mail service: attachment type blocking, anti-malware, sandboxing, URL rewriting and retroactive removal.
- DMARC report analysers (open-source parsers or hosted services): turn aggregate XML reports into a view of who sends mail as the enterprise.
- Remote browser isolation for high-risk roles (finance, executives, administrators) where budget allows.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
CISO / Head of Information Security	Approves filtering and attachment policies, TLS inspection rules and DMARC progression; reports on phishing exposure.
Messaging Administrator	Configures mail authentication, attachment blocking and anti-malware; handles quarantine releases.
Network / Security Engineer	Runs DNS and URL filtering, egress rules and gateway feed updates.
Endpoint Administrator	Manages browser and mail client versions and extension policies through endpoint management.
Domain / DNS Owner (often marketing or IT)	Maintains the register of domains and sending services and publishes DNS records.
DPO / Privacy Lead	Advises on lawful web monitoring and TLS inspection and employee notice.
All Users	Report suspicious mail and pages using the reporting button or channel.

M Documentation and Records

- Approved browser and email client standard

- Web and DNS filtering policy, including category list, TLS inspection rules and exception process
- Browser and mail extension allow-list and approval records
- Domain and email sending service register with SPF, DKIM and DMARC status
- Email attachment and anti-malware policy
- Quarantine release procedure

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 15-2. Assessment testing procedures, Control 9

Test ID	Method	Testing procedure	Result
TP-C09-01	SAMPLE	9.1: Select 25 end-user devices from the asset inventory across sites and operating systems. Record installed browsers and email clients and their versions; compare to the approved list and the vendor's current releases. Note unsupported, unapproved or outdated versions.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C09-02	INSPECT	9.1: Inspect endpoint management policies for browser and mail client updates. Confirm automatic updating is enforced, restart deferral is limited, and a mechanism detects or blocks unapproved browsers.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C09-03	RE-PERFORM	9.2: From an office device and a remote device on an external network, attempt to resolve a harmless test domain that the DNS filtering service publishes for testing (or a domain the enterprise has added to its block list). Confirm both lookups are blocked and logged.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C09-04	EXAMINE	9.2: Examine DNS filtering configuration and firewall rules. Confirm threat categories are enabled, all end-user devices are covered, and outbound DNS to other resolvers is restricted.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C09-05	RE-PERFORM	9.3: From a user device and a server, attempt to reach test URLs in blocked categories (using vendor-provided or safe test pages). Confirm the gateway blocks them and records the attempt; confirm servers are limited to required destinations.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C09-06	SAMPLE	9.3: Select ten URL filter exceptions or overrides granted in the last six months. Confirm each has a business justification, an approver and, where appropriate, an expiry.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C09-07	INSPECT	9.4: Inspect browser and mail client extension policies and an installed-extension report. Confirm an allow-list or deny-by-default policy is enforced and compare installed extensions on sampled devices with the approved list.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C09-08	RE-PERFORM	9.5: Query public DNS for SPF, DKIM and DMARC records for every domain in the domain register, including non-sending domains. Record the DMARC policy level, reporting addresses and any SPF errors (too many lookups, permissive endings).	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C09-09	EXAMINE	9.5: Examine three months of DMARC aggregate report summaries and the inbound gateway authentication policy. Confirm legitimate senders are aligned, unknown senders are investigated, and inbound mail failing DMARC is handled according to the sender's policy.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C09-10	RE-PERFORM	9.6: With the messaging administrator's agreement, send test messages from an external account carrying harmless files of blocked types (for example a renamed executable, a script, and an archive containing a disk image). Confirm they are blocked or quarantined by true file type.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C09-11	EXAMINE	9.7: Examine mail anti-malware and sandbox configuration, update status and detection reports for the last three months. Send an industry-standard anti-malware test file to confirm detection, and confirm retroactive removal is enabled and has been used.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Select devices from the asset inventory rather than the endpoint management console so unmanaged devices can surface, and include remote and field laptops, since DNS and web filtering often fail away from the office. Twenty-five devices suit a mid-sized enterprise; an IG1 firm with a few dozen devices can check all of them. For DMARC, test every domain in the register, not a sample, because unused domains are popular with spoofers. For filtering exceptions and quarantine releases, sample across the full review period. Use only harmless test files and test domains, agreed in advance, and record the agreement in the workpaper.

P Interview Questions

Interviewee	Question
Messaging Administrator	Which services send mail as your domains, and what is stopping you from moving DMARC to reject?
Network / Security Engineer	How are laptops protected by DNS and URL filtering when they are used at home or at a client site?
Endpoint Administrator	How would you know if a user installed a second browser or a new extension, and what happens next?
Finance Manager	Have you received mail that appeared to come from your own CEO or a supplier asking for a payment change? How was it handled?
DPO / Privacy Lead	Is TLS inspection used, which categories are exempt, and how were employees informed?

Q Technical and Process Verification

- Sampled devices run only approved, supported and current browsers and mail clients.
- DNS filtering blocks malicious domains on office and remote devices, and bypass is restricted.
- URL filtering covers all assets with an approved, maintained policy (IG2+).
- Extensions are controlled by allow-list; DMARC is published with progression to enforcement and inbound checks are on (IG2+).
- Unneeded attachment types are blocked by true type, and mail anti-malware with sandboxing is active and current (IG3).

R Expected Evidence

- Approved browser and mail client list and version reports
- DNS filtering configuration, enforcement settings and test results
- URL filtering policy, configuration and exception records
- Extension management policies and allow-list
- Domain register and DNS lookups for SPF, DKIM and DMARC
- DMARC aggregate report summaries
- Email gateway attachment and anti-malware configuration and test results
- Quarantine and detection reports

S Evaluation Criteria

Implemented

- Only supported, current browsers and clients run, and DNS filtering covers all end-user devices on and off the network (IG1).
- URL filtering, extension control, attachment blocking and DMARC with inbound checks are in place and maintained (IG2).
- Mail anti-malware with sandboxing is active, updated and monitored (IG3).

Partially implemented

- DNS or URL filtering protects office networks but not roaming devices.
- DMARC is published at p=none for a long period with no analysis of reports, or only the main domain is covered.
- Attachment blocking relies on file extensions only and misses archives.

Not implemented

- Users choose and update their own browsers; outdated and unsupported versions are common.
- No DNS or web filtering is in place.
- No SPF, DKIM or DMARC records, and no attachment controls beyond the mail provider's defaults.

T Common Gaps and Findings

- Condition: Laptops resolve DNS through home routers and public resolvers when off the office network. Criteria: 9.2 requires DNS filtering on all end-user devices, including remote ones. Effect: Malware and phishing domains are reachable for most of the working week for hybrid staff.
- Condition: DMARC has been at p=none for two years and nobody reads the reports. Criteria: 9.5 expects DMARC policy and verification to reduce spoofing. Effect: Attackers can send invoices from the enterprise's exact domain to its customers, and the enterprise does not see it.
- Condition: Users can install any browser extension. Criteria: 9.4 requires unnecessary and unauthorised extensions to be restricted. Effect: An extension with access to all sites can read session cookies for the ERP and cloud mail.
- Condition: The gateway blocks .exe attachments but passes ISO images and password-protected archives. Criteria: 9.6 requires blocking of unnecessary file types. Effect: Common malware delivery formats reach inboxes.
- Condition: Four marketing domains bought for campaigns have no SPF or DMARC records. Criteria: 9.5. Effect: Unused domains carrying the brand are easily used for convincing phishing.

U Remediation Guidance

- Deploy a DNS filtering agent or managed DNS profile to all laptops and mobiles through MDM, and block outbound DNS except to approved resolvers.
- Assign an owner for DMARC reports, fix alignment for legitimate senders, and move to quarantine then reject on a dated plan.
- Apply a deny-by-default extension policy with a small approved list and a request form; remove existing unapproved extensions.
- Extend attachment blocking to disk images, scripts, macro-enabled formats and archives, and quarantine password-protected archives for review.
- Publish SPF records with no permitted senders and DMARC reject for every non-sending domain, and add all domains to the register.

V Monitoring Metrics

- Percentage of devices running an approved browser at the current or previous release (target at least 98 percent).
- Percentage of end-user devices, including remote, protected by DNS filtering (target 100 percent).
- Percentage of owned domains with DMARC at quarantine or reject (target 100 percent within 12 months).
- Number of malicious messages caught at the gateway versus reported by users after delivery, per month.
- Phishing simulation click rate and report rate (linked to Control 14).

W Related Controls and Maturity Indicators

- Control 2 (software inventory and allow-listing of browsers and mail clients)
- Control 4 (secure configuration of browsers and mail clients)
- Control 7 (application patching keeps browsers current)
- Control 8 (DNS and URL logs, 8.6 and 8.7)
- Control 10 (malware defences on endpoints)
- Control 13 (network monitoring and defence)
- Control 14 (security awareness and phishing reporting)

Initial	Defined	Managed	Optimised
Users pick their own browsers, there is no filtering beyond the mail provider's defaults, and no one knows which services send mail as the enterprise.	An approved browser is managed and updated, DNS filtering protects the office, SPF and DMARC at monitoring are published, and some attachment types are blocked.	Filtering covers remote devices and servers, extensions are allow-listed, DMARC is enforced for all domains with reports analysed, attachments are blocked by true type, and metrics are reviewed monthly.	Mail is sandboxed with retroactive removal, high-risk users browse through isolation, filtering is tuned from SOC detections and threat intelligence, and phishing exposure trends inform training and investment.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A 300-employee Coimbatore textile exporter lost a large payment when a European buyer received an email, apparently from the exporter's own accounts address, asking for remittance to a new bank account. Investigation showed the domain had an SPF record but no DMARC, so the buyer's mail system accepted the forgery. At the same time, the exporter's own staff were receiving courier and GST-themed phishing daily, and the IT team found three browsers in use, some years out of date, and several coupon extensions with access to all websites. Using the CIS Controls as a checklist, the IT head worked through Control 9 over a quarter. Two mainstream browsers were approved and managed through the endpoint tool with automatic updates; other browsers were removed. A protective DNS service was configured on the office firewall and, through an agent, on the 60 laptops used by merchandisers who travel to buyer sites. The cloud mail suite's existing features were switched on: blocking of executables, scripts, disk images and macro-enabled files, quarantine of password-protected archives, and attachment sandboxing. DMARC was published at p=none, reports showed that a freight-forwarding portal and the ERP were sending mail as the exporter without alignment, and after those were fixed the policy moved to reject within ten weeks. The exporter also told its main buyers about the change and agreed a call-back rule for bank-detail changes. No further spoofing incidents were reported, and the exporter noted the incident in its CERT-In and insurer records as required.

WP-C09: use the workpaper format shown in Appendix H.

CHAPTER 16 · CIS CONTROL 10

Malware Defenses

CIS CONTROL 10 · 7 SAFEGUARDS · 3 IN IG1

Malware Defenses

CIS Controls v8.1 · titles quoted verbatim | WP-C10

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 10 — Malware Defenses

Control 10 is about stopping hostile code from installing itself, running or spreading on enterprise assets, and about noticing quickly when it gets through. It covers the classic anti-malware agent with automatically refreshed detection content, closing the old removable-media doors (auto-execution and unscanned USB drives), switching on the exploit mitigations that modern operating systems already ship with, running the whole capability from one console, and using detection that judges behaviour rather than only known file fingerprints. Malware here is a broad term: ransomware, information stealers, remote access trojans, loaders, cryptominers, worms and malicious scripts all fall within it. The Control does not ask for any particular product. In practice many enterprises meet most of it with an endpoint detection and response (EDR) platform or with the protection built into their operating system, provided it is centrally managed and its health is watched. Control 10 sits alongside Control 2 (allowlisting reduces what can run at all), Control 4 (secure configuration), Control 7 (patching removes the flaws exploits target) and Control 9 (email and browsers are the main delivery routes).

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 16-1. Safeguards of CIS Control 10, Malware Defenses

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
10.1	**“Deploy and Maintain Anti-Malware Software”**	Devices	Detect	IG1	Every enterprise asset that can run malicious code (laptops, desktops, servers, virtual machines and, where the platform supports it, mobile devices) carries an anti-malware agent that is installed, running, licensed and kept healthy for as long as the asset is in service.
10.2	**“Configure Automatic Anti-Malware Signature Updates”**	Devices	Protect	IG1	Detection content (signature files, definition packs and the cloud intelligence the engine relies on) refreshes automatically on every protected asset without waiting for a user or administrator to act, so that protection keeps pace with newly catalogued threats.
10.3	**“Disable Autorun and Autoplay for Removable Media”**	Devices	Protect	IG1	Operating systems are configured so that inserting a USB stick, external drive, memory card or optical disc never launches content on its own; anything on the media runs only if a user deliberately opens it.
10.4	**“Configure Automatic Anti-Malware Scanning of Removable Media”**	Devices	Detect	IG2	When removable media is attached, the anti-malware engine examines its contents straight away and blocks or quarantines anything harmful before the user can open it.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
10.5	**“Enable Anti-Exploitation Features”**	Devices	Protect	IG2	Built-in exploit mitigations in the operating system and in key applications (memory protections, code-integrity checks, application sandboxing and platform integrity features) are switched on wherever the platform and the application can tolerate them, making it harder for an attacker to turn a software flaw into running code.
10.6	**“Centrally Manage Anti-Malware Software”**	Devices	Protect	IG2	Anti-malware agents are administered from a central console that sets policy, pushes updates, collects alerts and shows the health of every agent, rather than being configured device by device.
10.7	**“Use Behavior-Based Anti-Malware Software”**	Devices	Detect	IG2	The anti-malware capability goes beyond matching known files: it watches what processes actually do (encryption bursts, credential dumping, unusual parent-child chains, script abuse) and can stop or flag activity that looks malicious even when no signature exists.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
10.1	**1.** Reconcile the asset inventory from Control 1 against the anti-malware console so that every in-scope asset has an agent, and record a justified exception for any platform where no agent exists (for example an appliance or an OT controller). **2.** Build the agent into every gold image, cloud template and device-enrolment profile so that new assets are protected from first boot rather than after a manual install. **3.** Protect the agent from tampering: require a password or console approval to uninstall or disable it, and alert when the agent stops reporting. **4.** Track licence counts and agent versions so that expiry or an unsupported build is spotted before protection lapses.	• Console export listing protected assets, agent version and last check-in, reconciled to the asset inventory. • Approved exception register for assets without an agent, with the compensating control for each. • Gold image or enrolment profile showing the agent as a mandatory component.
10.2	**1.** Set the update policy in the console to pull new definitions several times a day, with a fallback source for assets that are off the corporate network. **2.** Prevent users from deferring or switching off updates through the local interface. **3.** Define an age threshold (for example definitions older than 72 hours) and raise an alert or ticket for any asset that crosses it. **4.** For isolated or air-gapped segments, document a controlled offline update route with a named owner and a fixed cadence.	• Update policy configuration showing automatic, user-locked updates. • Report of definition age across the estate on the test date, with stale assets highlighted. • Procedure and log for offline updates in isolated networks, where relevant.

Safeguard	Practical steps	Evidence
10.3	**1.** Apply a central configuration setting (group policy, MDM profile or configuration script) that turns off automatic execution and automatic playback for all drive types. **2.** Include the setting in the secure configuration baseline from Control 4 so that drift is detected by the same compliance checks. **3.** Verify the setting on a sample of assets after build and after major operating system upgrades, which sometimes reset defaults.	• Exported policy or profile showing auto-execution disabled for all media types. • Configuration compliance report for the setting across the estate. • Spot-check record from a sampled workstation.
10.4	**1.** Enable on-insertion and on-access scanning for removable drives in the central anti-malware policy. **2.** Decide what happens on detection: block access, quarantine the file and notify the security team, and record that decision in the policy. **3.** Where the business allows, pair scanning with device control so that only approved or encrypted media can be mounted at all. **4.** For shop-floor or laboratory systems that need USB transfers, provide a dedicated scanning kiosk and require its use.	• Anti-malware policy showing removable-media scanning enabled. • Console events from a test insertion or a real detection on removable media. • Device control policy or kiosk procedure, where used.
10.5	**1.** List the mitigations each supported platform offers, such as data execution prevention, address space layout randomisation, control-flow protections, attack surface reduction rules, macOS System Integrity Protection and Gatekeeper, and Linux mandatory access control. **2.** Enable them centrally, starting in audit mode for rules likely to break line-of-business software, then move to enforcement once the impact is understood. **3.** Record any application-specific exclusion with an owner, a reason and a review date. **4.** Recheck the mitigation state after operating system upgrades and major application releases.	• Platform-by-platform mitigation baseline showing the intended state. • Configuration export or compliance report showing mitigations enforced. • Exclusion register with approvals and review dates.
10.6	**1.** Enrol all agents into a single management console (on-premises or cloud-hosted) and remove locally managed or standalone installations. **2.** Group assets by role (servers, laptops, kiosks, OT gateways) and apply policy per group, with changes made only through the console and recorded. **3.** Restrict console administration to named individuals with multi-factor authentication, and log console changes. **4.** Forward detections and agent-health events to the SIEM or log platform so that they are correlated with other telemetry under Control 8.	• Console screenshot or export showing all agents managed centrally and grouped by policy. • Console administrator list and MFA setting. • Evidence that detections reach the central log platform, such as a sample forwarded alert.

Safeguard	Practical steps	Evidence
10.7	**1.** Confirm that the deployed product includes behavioural, heuristic or machine-learning detection and that it is switched on rather than merely licensed. **2.** Set the response mode for high-confidence behaviours, such as ransomware-like file encryption, to block and isolate, and for lower-confidence behaviours to alert. **3.** Assign someone to triage behavioural alerts within a defined time, because these detections lose value if nobody looks at them. **4.** Test the capability periodically with a safe simulation (for example a benign ransomware or credential-theft emulation) and record the outcome.	• Policy export showing behavioural protection enabled and its response mode. • Sample of behavioural alerts with triage notes and closure. • Record of a periodic detection test and its result.

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
An IG1 enterprise must have working anti-malware on every asset that can run it (10.1), with detection content that updates by itself (10.2), and must disable auto-execution for removable media (10.3). For a 40-person firm this can be as simple as the protection built into the operating system, managed through a cloud console or MDM, plus one group policy or profile setting for autorun. The test is coverage and freshness, not product sophistication.	IG2 adds automatic scanning of removable media (10.4), enabling exploit mitigations on assets and software (10.5), central management of the anti-malware estate (10.6) and behaviour-based detection (10.7). Together these move the enterprise from file-matching on each device to a managed capability that sees attacker behaviour and can be supervised from one place, which is what an organisation with servers, remote staff and sensitive data needs.	No IG3-only Safeguards; IG3 enterprises apply all seven Safeguards with more rigour: near-complete coverage including servers, cloud workloads and specialised platforms, tight exclusion governance, enforced attack surface reduction rules, round-the-clock alert triage (in-house or through a managed detection service), regular adversary emulation to test detection, and integration of endpoint telemetry with threat hunting and incident response.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 10.1 → 8.7 Protection against malware; 8.1 User endpoint devices
- 10.2 → 8.7 Protection against malware; 8.8 Management of technical vulnerabilities (supporting)
- 10.3 → 8.7 Protection against malware; 7.10 Storage media; 8.9 Configuration management
- 10.4 → 8.7 Protection against malware; 7.10 Storage media
- 10.5 → 8.7 Protection against malware; 8.9 Configuration management; 8.8 Management of technical vulnerabilities
- 10.6 → 8.7 Protection against malware; 8.15 Logging; 8.16 Monitoring activities
- 10.7 → 8.7 Protection against malware; 8.16 Monitoring activities; 5.7 Threat intelligence (supporting)

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: DE.CM-09 (computing hardware, software and runtime environments monitored for adverse events); PR.PS-01 (configuration management); PR.PS-02 (software maintained); DE.AE-02 (adverse events analysed) — Srida IT mapping
- NIST SP 800-53 Rev. 5: SI-3 Malicious Code Protection; SI-4 System Monitoring; SI-16 Memory Protection; MP-7 Media Use; CM-7 Least Functionality
- MITRE ATT&CK: behaviour-based detection maps to many techniques, including T1486 Data Encrypted for Impact and T1003 OS Credential Dumping; useful for testing 10.7
- PCI DSS v4.0.1: Requirement 5 (protect systems and networks from malicious software), where cardholder data is in scope

F India Regulatory Touchpoints

- CERT-In Directions of 28 April 2022: malware, malicious code and ransomware attacks are among the reportable incident types, to be reported within 6 hours of noticing; endpoint detections are often the first evidence.
- RBI cyber security framework and IT governance directions for banks and NBFCs: expect anti-malware protection, centralised monitoring and timely detection on endpoints and servers.
- SEBI Cybersecurity and Cyber Resilience Framework (CSCRF, 2024): regulated entities are expected to deploy endpoint protection and, for larger categories, EDR-type capability feeding security operations.
- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6: reasonable security safeguards to prevent personal data breach; a malware-driven breach may also trigger intimation duties under r.7.

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Most serious intrusions involve malicious code at some stage. A user opens a booby-trapped attachment or downloads a fake installer, a loader fetches a remote access tool, the attacker steals credentials and moves sideways, and the final stage is often ransomware or quiet data theft. Each of those stages leaves behaviour that a healthy, centrally watched endpoint agent can see and often stop. Where the agent is missing, out of date or disabled by a user, the attacker works unobserved, and the first sign of trouble is frequently the ransom note.

Failure in this Control is rarely about having no anti-malware at all. It is usually about the gaps: the forty servers never enrolled in the console, the laptop whose definitions are three months old because it never connects to the office network, the exclusion added for a slow application that turned out to cover an entire drive, or the alert that fired at 2 a.m. and was read nine days later. The consequences are business outage, regulatory reporting, recovery cost and, where personal data is stolen, exposure under data protection law.

In India, malware and ransomware incidents are squarely within the categories CERT-In expects to be reported, and its April 2022 Directions set a short reporting window. Regulated entities face sector expectations from RBI, SEBI and IRDAI that include endpoint protection and timely detection. Indian SMEs, which often run unmanaged consumer antivirus, unlicensed software and shared USB drives on shop floors and in accounts offices, are a frequent target, and an incident at a small supplier can travel up the supply chain to a larger customer.

I Applicability

Control 10 applies to every enterprise. A 40-person Kochi CA firm can meet IG1 with the operating system's built-in protection managed from a cloud console, automatic updates and a single autorun setting; the main risk for such firms is unmanaged personal laptops and shared USB drives carrying client files. Cloud and SaaS-heavy start-ups still need agents on staff laptops and on any cloud virtual machines or container hosts they run; for serverless and fully managed SaaS, the provider carries the endpoint layer and the enterprise should confirm this in the shared-responsibility model (Control 15). In OT environments, such as a Chennai auto-parts plant, controllers and older HMIs often cannot run an agent or accept frequent updates; there the enterprise protects the engineering workstations and historians, uses USB scanning kiosks, and records the unprotected devices as exceptions with network isolation as the compensating control (Control 12 and Control 13). Where IT is outsourced to an MSP, the enterprise remains accountable: it should see the console reports, know the coverage and alert-handling times, and have them in the contract.

J Implementation Guidance

1. Agree the scope: every asset class in the Control 1 inventory, the platforms each runs, and which product or built-in capability will protect each. Record platforms that cannot run an agent and the compensating control.
2. Select or confirm a centrally managed endpoint protection capability with behavioural detection. For many IG2 enterprises an EDR platform covers 10.1, 10.2, 10.6 and 10.7 together.
3. Deploy the agent through gold images, MDM enrolment and cloud templates, then sweep for unprotected assets by reconciling the console against the inventory and network discovery results.
4. Set policy per asset group: automatic updates, tamper protection, on-access and removable-media scanning, response actions for high-confidence detections, and a strict, reviewed exclusion list.
5. Disable auto-execution for removable media through the configuration baseline and, where the business can accept it, add device control to limit which media can mount.

6. Enable exploit mitigations platform by platform, starting in audit mode where software compatibility is uncertain, and move to enforcement on a dated plan.
7. Connect detections and agent-health events to the SIEM or log platform and define who triages them, within what time, and how they escalate into incident response (Control 17).
8. Monitor health continuously: coverage percentage, definition age, agents not reporting, exclusions and disabled protection, with a weekly review and tickets for exceptions.
9. Test detection at least annually, and after major changes, with safe simulations of common attacker behaviour, and record results and fixes.
0. Review the whole Control yearly with the risk owner, including exclusions, unprotected platforms and the performance of any MSP or managed detection provider.

K Tools and Automation

- Endpoint protection platform or EDR: provides the agent, automatic content updates, behavioural detection, isolation and a central console; covers most of the Control in one place.
- Built-in operating system protection managed through MDM or a cloud console: often sufficient for IG1 in small firms when coverage and updates are watched.
- Mobile device management (MDM) and configuration management tools: deploy agents, enforce autorun and exploit-mitigation settings, and report configuration compliance.
- SIEM or log platform (for example Wazuh as an open-source option): collects detections and agent-health events and correlates them with network and identity logs.
- Endpoint query and forensics tools (for example osquery or Velociraptor): verify agent presence and settings across the estate and support investigation after a detection.
- Device control and USB scanning kiosks: limit which removable media can be used and scan media before it reaches sensitive or OT systems.
- Adversary emulation frameworks (open-source, used safely in a test group): exercise behavioural detection to confirm it fires as expected.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
IT operations / endpoint team	Deploys and maintains agents, policies and exploit mitigations; resolves coverage and update exceptions.
Security operations (in-house or managed)	Triages detections and behavioural alerts within agreed times; escalates incidents; tunes detection.
CISO / information security manager	Owns the malware defence standard, approves exclusions and exceptions, reports coverage and incidents to management.
Asset owners and application owners	Confirm business impact of mitigations, justify exclusions and accept residual risk for unprotected platforms.
OT / plant engineering lead	Agrees protection approach for industrial systems, operates USB kiosks and offline update routes.
MSP or managed detection provider	Delivers contracted monitoring and response, provides coverage and response-time reports to the enterprise.

M Documentation and Records

- Malware defence standard: scope, required capabilities per platform, update and scanning rules, response modes.
- Anti-malware policy configuration per asset group, exported and version-controlled.
- Exclusion and exception register with owner, justification, compensating control and review date.
- Removable media and device control procedure, including USB kiosk use for OT and labs.
- Exploit mitigation baseline per platform, part of the Control 4 configuration baselines.
- Alert triage and escalation runbook linked to the incident response plan.
- Detection test records and annual Control review minutes.

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 16-2. Assessment testing procedures, Control 10

Test ID	Method	Testing procedure	Result
TP-C10-01	EXAMINE	10.1: Examine the malware defence standard and confirm it defines scope (all asset types that can run an agent), required capability per platform and the handling of assets that cannot be protected.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-02	RE-PERFORM	10.1: Re-perform a reconciliation of the asset inventory against the anti-malware console on the test date. Calculate coverage for workstations, servers and cloud workloads separately, and list every unprotected asset without an approved exception.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-03	SAMPLE	10.1: Select a sample of assets (including recently built assets and servers) and inspect each locally to confirm the agent is installed, running, tamper-protected and reporting to the console.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-04	INSPECT	10.2: Inspect the update policy to confirm updates are automatic, frequent and cannot be turned off by users. Obtain the definition-age report and identify assets whose content is older than the enterprise's threshold; for a sample of these, check whether tickets were raised and resolved.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-05	SAMPLE	10.2: For a sample of weeks across the review period, obtain historical health reports or console snapshots and confirm stale-definition exceptions were identified and corrected within the defined time, demonstrating operation over time rather than on one day.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-06	INSPECT	10.3: Inspect the group policy, MDM profile or configuration script that disables auto-execution for all removable drive types, and the configuration compliance report showing its application across the estate.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-07	OBSERVE	10.3: On a sampled workstation, observe the insertion of a test USB drive containing a harmless autorun file and confirm nothing launches automatically.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-08	OBSERVE	10.4: Using a test drive holding an industry-standard anti-malware test file, observe that the engine scans the media on insertion and blocks or quarantines the file, and that the event appears in the central console.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-09	INSPECT	10.5: Inspect the exploit mitigation baseline and configuration exports for each platform in scope, and confirm mitigations are in enforcement mode. Examine the exclusion register for approvals, justifications and current review dates.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-10	INSPECT	10.6: Inspect the central console to confirm all agents are managed from it, that policies are applied by group, and that no standalone or locally managed installations remain. Review the console administrator list, its MFA setting and the console change log for a sample of policy changes.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-11	EXAMINE	10.6: Examine evidence that detections and agent-health events are forwarded to the SIEM or log platform, by tracing a sample of console alerts to their central log records.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-12	INSPECT	10.7: Inspect policy settings to confirm behavioural or heuristic protection is enabled and set to block for high-confidence behaviours such as ransomware-like encryption.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C10-13	SAMPLE	10.7: Select a sample of behavioural alerts from across the review period and confirm each was triaged within the defined time, with a recorded outcome and, where warranted, escalation to incident response.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C10-14	**INTERVIEW**	10.7: Interview the security operations lead about the most recent detection test or adversary emulation, and examine its record to confirm what fired, what did not and what was fixed.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Sample across asset types and locations rather than from one convenient group: include servers, remote laptops that rarely touch the office network, newly built assets, cloud virtual machines and any OT engineering workstations. For an estate under 100 assets, test 5 to 10 assets individually; for larger estates, 20 to 25 is usually enough, supported by a full-population reconciliation of the console against the inventory, which is cheap to re-perform and far more telling than any sample. For operating effectiveness, pick at least four points spread over the review period (for example one week per quarter) and confirm that health exceptions and alerts were handled within the defined times. Sample behavioural alerts from different severities, including at least one out-of-hours alert.

P Interview Questions

Interviewee	Question
IT operations / endpoint team	How do you know a newly built server or laptop has the agent, and what happens if one turns up in discovery without it?
IT operations / endpoint team	Who can add an exclusion, how is it approved, and when were exclusions last reviewed?
Security operations	Walk me through the last behavioural alert: when it fired, who looked at it, how long it took and what was done.
CISO	Which platforms cannot run an agent, and how is the risk from them reduced and accepted?
OT / plant engineering lead	How do files reach plant systems on removable media, and how are those media checked first?
MSP or managed detection provider	What coverage and response-time reports do you give the enterprise, and how often?

Q Technical and Process Verification

- Coverage reconciliation from inventory to console shows all in-scope assets protected or excepted.
- Definition age across the estate is within threshold, with stale assets ticketed.
- Auto-execution disabled and removable media scanned, confirmed by live test.
- Exploit mitigations enforced per baseline, with governed exclusions.
- Single central console, restricted administration and alerts forwarded to central logging.
- Behavioural detection enabled, alerts triaged on time and tested periodically.

R Expected Evidence

- Malware defence standard and exception register.
- Console export of protected assets reconciled to the asset inventory.
- Update policy and definition-age report, with historical snapshots.
- Autorun configuration and compliance report; USB test record.
- Removable-media scanning policy and test detection event.
- Exploit mitigation baseline, configuration exports and exclusion approvals.
- Console administrator list, MFA setting and change log.
- Sample of behavioural alerts with triage records.
- Detection test or adversary emulation report.

S Evaluation Criteria

Implemented

- All in-scope assets run a centrally managed, tamper-protected agent with current content, and every exception is approved with a compensating control.
- Autorun is disabled and removable media is scanned automatically, confirmed by testing.
- For IG2 and above, exploit mitigations are enforced and behavioural detection is enabled, with alerts triaged within defined times throughout the period.

Partially implemented

- Agents exist on most assets but servers, cloud workloads or remote laptops are missing or out of date.
- Central management or behavioural detection is licensed but not fully configured, or alerts are not reviewed promptly.
- Exploit mitigations are in audit mode with no dated plan to enforce.

Not implemented

- No anti-malware on a significant part of the estate, or only unmanaged consumer products with no visibility.
- Definitions are not updated automatically, or autorun remains enabled.
- No one reviews detections, so alerts go unseen.

T Common Gaps and Findings

- Condition: 38 of 210 servers are absent from the anti-malware console. Criteria: 10.1 requires anti-malware on all enterprise assets. Effect: attackers who reach these servers can stage ransomware without detection.
- Condition: remote laptops show definitions up to 60 days old because updates come only from an on-premises server. Criteria: 10.2 requires automatic updates on every asset. Effect: newer malware families go undetected on the most exposed devices.
- Condition: an exclusion for an accounting package covers the entire D: drive. Criteria: 10.5 and 10.6 expect controlled, narrow exclusions. Effect: malware placed in that drive is never scanned.
- Condition: behavioural alerts are emailed to a shared mailbox reviewed weekly. Criteria: 10.7 expects behaviour-based detection to be acted on. Effect: an intrusion can progress for days before anyone responds.
- Condition: plant HMIs receive files on personal USB drives with no scanning. Criteria: 10.3 and 10.4 address removable-media risk. Effect: malware can bypass network defences and reach production systems.
- Condition: the MSP contract does not specify alert response times or coverage reporting. Criteria: 10.6 central management, supported by Control 15 provider oversight. Effect: the enterprise cannot show that the Control operates.

U Remediation Guidance

- Run a full reconciliation of inventory against console, deploy agents to every missing asset within 30 days and make reconciliation a weekly automated report.
- Move to cloud-delivered or internet-reachable updates for off-network devices and alert on definition age above 72 hours.
- Replace broad exclusions with narrow, file- or process-specific ones approved by the CISO, and review all exclusions quarterly.
- Route behavioural alerts into the SIEM or ticketing system with severity-based response targets, using a managed detection service if out-of-hours cover is not possible in-house.
- Install a USB scanning kiosk for plant transfers, enforce device control on HMIs where feasible, and document the remaining exceptions.
- Amend the MSP contract to include coverage, update and alert-response measures reported monthly.

V Monitoring Metrics

- Agent coverage: percentage of in-scope assets with a healthy, reporting agent (target 98% or higher, with 100% of servers).
- Definition freshness: percentage of assets with content less than 72 hours old.
- Mean time to triage high-severity behavioural alerts (target set by the enterprise, for example under 1 hour).
- Number of open exclusions, and percentage reviewed within the last quarter.
- Detection test pass rate: share of emulated behaviours detected or blocked in the latest test.

W Related Controls and Maturity Indicators

- Control 1 (asset inventory for coverage reconciliation)
- Control 2, especially 2.5 to 2.7 (allowlisting limits what can run)

- Control 4 (secure configuration baselines carry autorun and mitigation settings)
- Control 7 (patching removes the flaws exploits target)
- Control 8 (central collection of detections)
- Control 9 (email and web filtering block common delivery routes)
- Control 13 (network monitoring complements endpoint detection)
- Control 17 (incident response for confirmed infections)

Initial	Defined	Managed	Optimised
Anti-malware is installed ad hoc, often consumer products, with no central view; updates and autorun depend on each device.	A malware defence standard exists; a central console manages most assets; autorun and update settings are part of the baseline; exceptions are recorded.	Coverage, freshness and alert-handling are measured weekly against targets; exploit mitigations are enforced; behavioural alerts are triaged within agreed times and feed incident response.	Detection is tested regularly against current attacker behaviour, tuned from incident and threat intelligence lessons, and integrated with automated containment and threat hunting.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A 600-employee Pune NBFC ran a well-known anti-malware product on its branch desktops, but an internal review before its RBI inspection found three problems. The console listed 540 devices while the asset inventory listed 690; most of the difference was loan-processing servers and a group of field-officer laptops that synchronised definitions only when they visited a branch. Behavioural protection had been licensed for two years but left in alert-only mode, and alerts went to an inbox the two-person IT team checked on Mondays. And the collections team routinely brought documents in on USB drives, with autorun still enabled on older images.

The CISO treated it as a Control 10 project with a 60-day plan. The team replaced the old product with a centrally managed EDR capability, pushed it through the device-management tool and the server build scripts, and set a weekly report reconciling the console to the asset inventory. Laptops were moved to cloud-delivered updates with an alert for anything older than 72 hours. A group policy disabled autorun for all drive types, removable-media scanning was enforced, and exploit-mitigation rules ran in audit mode for three weeks before enforcement, which surfaced one legacy document-scanning tool that needed a narrow exclusion approved by the CISO.

Because the NBFC could not staff a night shift, it contracted a managed detection service with a 30-minute response target for high-severity alerts, written into the contract along with a monthly coverage report. Two months later the service isolated a field laptop where a fake courier-tracking attachment had launched a credential-stealing script; the behavioural engine blocked the script and the laptop was rebuilt the same day. The incident was assessed against the CERT-In reporting criteria and logged, and the assessor at the next review rated all seven Safeguards Implemented.

WP-C10: use the workpaper format shown in Appendix H.

CHAPTER 17 · CIS CONTROL 11

Data Recovery

CIS CONTROL 11 · 5 SAFEGUARDS · 4 IN IG1

Data Recovery

CIS Controls v8.1 · titles quoted verbatim | WP-C11

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 11 — Data Recovery

Control 11 makes sure that when data is lost, corrupted or encrypted, the enterprise can put it back to a known good state within a time the business can live with. It asks for four things in practice: a written recovery process with priorities and objectives, automated backups at a frequency the data deserves, protection of backups to the same standard as the original data, and at least one copy that is isolated from the production environment. Enterprises at IG2 and above must also prove recovery works by restoring samples every quarter. Data recovery is not the same as business continuity or disaster recovery for whole sites, although it underpins both; it is the narrower, testable capability to get data back. In the current threat landscape, Control 11 is above all a ransomware control: attackers routinely seek out and destroy backups before encrypting production, so the value of this Control depends on whether the backups survive an attacker who already holds administrator rights.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 17-1. Safeguards of CIS Control 11, Data Recovery

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
11.1	**“Establish and Maintain a Data Recovery Process”**	Documentation	Govern	IG1	The enterprise writes down how it will get its data back: which systems and data are covered, in what order they are restored, how fast and to what point in time, who does it, and how the backups themselves are kept safe. The document is reviewed at least once a year and whenever a significant change (a new core system, a cloud migration, an acquisition) could affect it.
11.2	**“Perform Automated Backups”**	Data	Recover	IG1	Backups of in-scope systems and data run on a schedule without anyone having to start them, at least once a week and more often where the data changes quickly or matters more, and failures are noticed and fixed.
11.3	**“Protect Recovery Data”**	Data	Protect	IG1	Backup copies receive at least the same protection as the live data they hold: if the production data is confidential or personal, the backup is too, so it is encrypted, access-controlled and monitored to the same standard or better.
11.4	**“Establish and Maintain an Isolated Instance of Recovery Data”**	Data	Recover	IG1	At least one copy of recovery data is kept apart from the production environment so that an attacker or failure that destroys the live systems cannot also reach it: for example an offline or air-gapped copy, an immutable or versioned cloud store, or an off-site copy under different credentials.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
11.5	**“Test Data Recovery”**	Data	Recover	IG2	At least every quarter, the enterprise actually restores a sample of in-scope systems or data from backup and checks that the result is complete, usable and achieved within the agreed recovery times.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
11.1	**1.** Build a recovery scope from the asset and data inventories (Controls 1 and 3), classifying each system by business criticality and setting a recovery time objective (RTO) and recovery point objective (RPO) agreed with its owner. **2.** Set a restoration order that reflects dependencies: identity services, DNS and network first, then core business applications, then the rest. **3.** Describe backup security in the process: encryption, access restrictions, separation of backup credentials from production, and the isolated copy required by 11.4. **4.** Assign named owners, schedule an annual review and list the change triggers that force an earlier one.	• Approved data recovery process document with version history and last review date. • Recovery scope register listing systems, owners, RTO, RPO and restoration priority. • Record of the latest review, including changes made after a significant enterprise change.
11.2	**1.** Configure backup jobs in a backup platform or cloud service for every system in the recovery scope, with frequency set by the RPO (for example nightly for finance databases, hourly log backups for core transaction systems, weekly for static file shares). **2.** Include SaaS data (email, collaboration, CRM) and cloud workloads, which are often wrongly assumed to be backed up by the provider. **3.** Alert on failed, skipped or partial jobs and require a ticket and resolution for each. **4.** Reconcile the backup job list against the recovery scope quarterly so that new systems are not silently left out.	• Backup job configuration showing schedules and targets for each in-scope system. • Job success and failure reports over the review period, with tickets for failures. • Quarterly reconciliation of jobs to the recovery scope.
11.3	**1.** Encrypt backups at rest and in transit, and store the encryption keys separately from the backup media, with a documented key recovery route. **2.** Restrict backup console and storage access to a small set of named administrators using accounts that are separate from everyday and domain administrator accounts, protected by multi-factor authentication. **3.** Log access to the backup system and to restored data, and review it. **4.** Apply the same retention and disposal rules to backups as to the source data, including obligations to erase personal data once its purpose has ended.	• Backup encryption settings and key management record. • Access list for the backup platform and storage, with MFA configuration. • Access logs and retention policy for backup data.

Safeguard	Practical steps	Evidence
11.4	**1.** Choose an isolation method suited to the enterprise: offline media rotated off-site, immutable object storage with a retention lock, a separate cloud account or tenancy, or a provider vault that cannot be deleted from the production side. **2.** Ensure the isolated copy uses credentials and administrative paths that are not shared with the production directory, so that a compromised domain administrator cannot delete it. **3.** Keep several restore points (versioning) so that a copy taken after silent encryption or corruption is not the only option. **4.** Verify the isolation itself periodically, for example by confirming that deletion attempts from production credentials fail.	• Architecture or configuration showing the isolated copy, its retention lock or offline status and its separate credentials. • Media rotation log or immutable-storage configuration with retention period. • Record of a test showing the isolated copy cannot be altered from production.
11.5	**1.** Plan a rolling quarterly test schedule so that, over a year, every critical system is restored at least once and the isolated copy from 11.4 is used in at least one test. **2.** Restore into a safe environment, have the business owner confirm the data is complete and usable, and time the exercise against the RTO and RPO. **3.** Record failures and lessons learned, fix them, and retest. **4.** Include at least one scenario per year that assumes ransomware, in which production identity and backup servers are unavailable.	• Quarterly restore test plan and completed test reports with timings. • Business-owner sign-off that restored data is usable. • Remediation records for failed tests and retest results.

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
Four of the five Safeguards are IG1, which shows how central recovery is to essential hygiene. Every enterprise must document its recovery process (11.1), run automated backups at least weekly (11.2), protect backup data as well as the original (11.3) and keep an isolated copy (11.4). For a small firm this can mean a cloud backup service for laptops and SaaS, plus an immutable or offline copy, with a two-page procedure that says what is backed up and how to restore it.	IG2 adds quarterly restore testing of a sample of in-scope assets (11.5). This is the step that turns backups into proven recoverability, and it should cover timings against RTO and RPO, business confirmation of usable data and at least one test from the isolated copy.	No IG3-only Safeguards; IG3 enterprises apply all five Safeguards with more rigour: tighter RPOs with continuous or near-continuous protection for critical data, full ransomware recovery exercises including rebuilding identity services from clean media, a clean-room or isolated recovery environment, integrity scanning of backups before restore, and recovery results reported to the board.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 11.1 → 8.13 Information backup; 5.30 ICT readiness for business continuity; 5.29 Information security during disruption
- 11.2 → 8.13 Information backup
- 11.3 → 8.13 Information backup; 8.24 Use of cryptography; 5.33 Protection of records; 7.10 Storage media
- 11.4 → 8.13 Information backup; 5.30 ICT readiness for business continuity
- 11.5 → 8.13 Information backup; 5.30 ICT readiness for business continuity; Clause 9.1 Monitoring, measurement, analysis and evaluation

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: PR.DS-11 (backups of data are created, protected, maintained and tested); RC.RP-01 to RC.RP-03 (recovery plan executed, recovery actions selected, integrity of backups verified before restoration) — Srida IT mapping

- NIST SP 800-53 Rev. 5: CP-9 System Backup; CP-10 System Recovery and Reconstitution; CP-4 Contingency Plan Testing; CP-6 Alternate Storage Site
- ISO 22301:2019 business continuity management: Control 11 provides the data-recovery capability that continuity plans depend on
- Common practice reference: the 3-2-1 backup rule (three copies, two media types, one off-site), often extended to 3-2-1-1-0 (one immutable or offline copy, zero restore errors in testing); an industry convention, not a CIS requirement

F India Regulatory Touchpoints

- RBI IT governance and cyber security directions for banks and NBFCs: expect documented backup and restoration policies, periodic restore testing and business continuity and disaster recovery drills.
- SEBI CSCRF (2024): sets expectations on backup, recovery and recovery time objectives for regulated entities, stricter for market infrastructure institutions.
- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6: reasonable security safeguards for personal data, with data backups and measures for continued processing after compromise listed among them.
- CERT-In Directions of 28 April 2022: ransomware incidents must be reported within 6 hours of noticing; recovery evidence also supports the incident report.

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Ransomware crews have learned that a victim with good backups does not pay. Their playbook therefore includes a deliberate hunt for the backup console, the backup service accounts and any network-attached backup storage, followed by deletion of restore points and shadow copies before encryption starts. Enterprises that kept backups on the same domain, reachable with the same administrator credentials, often discover that every copy was destroyed in the same hour as production. An isolated, versioned copy that the production domain cannot touch is what turns a crisis into a recovery.

Backup failures that have nothing to do with attackers are just as common: jobs that have failed quietly for months, a new system never added to the schedule, SaaS mailboxes everyone assumed the provider protected, encryption keys stored on the server that was lost, or a restore that technically works but takes eleven days against a two-day business tolerance. None of these is visible until a restore is attempted, which is why regular testing matters more than the backup software itself.

In India, ransomware has hit hospitals, ports, power utilities, financial institutions and many SMEs, and regulators have responded. RBI, SEBI and IRDAI expect regulated entities to maintain tested backup and recovery arrangements, and SEBI CSCRF sets recovery expectations for market entities. The DPDP Rules 2025 list backups and continuity of processing among reasonable security safeguards for personal data. A 40-person firm that loses its accounting data loses its business; a hospital chain that cannot restore patient records puts lives at risk.

I Applicability

Control 11 applies to every enterprise, whatever its size. A 40-person Kochi CA firm with client ledgers, tax filings and email in SaaS needs a third-party backup of that SaaS data, a backup of any local accounting server, and one copy the office network cannot reach; the owner or the outsourced IT provider should restore a sample file every quarter even though 11.5 is formally IG2. Cloud-first start-ups must not assume the cloud provider backs up their data: shared responsibility usually leaves backup, versioning and cross-account copies with the customer. Enterprises with OT, such as a Chennai auto-parts maker, must back up PLC programs, HMI projects, historian data and engineering workstation images, and keep known-good copies offline because plant systems often cannot be rebuilt from vendor media quickly. Where an MSP runs backups, the enterprise should hold the restore test reports, know where the isolated copy is and make sure the MSP's own credentials cannot delete it, since MSP compromise is a known ransomware route.

J Implementation Guidance

1. Identify what must be recoverable: use the asset and data inventories to list systems, SaaS tenants, databases, file stores, configurations (including network device configurations from Control 12) and OT projects.
2. Agree RTO and RPO with business owners for each critical system, and set the restoration order based on dependencies, starting with identity, DNS, network and backup infrastructure itself.

3. Write the data recovery process covering scope, frequency, retention, security of backups, isolation, roles, restoration steps and testing; approve it and set an annual review.
4. Deploy or confirm automated backups for every in-scope item, with frequencies driven by RPO, and alerting on failure.
5. Harden the backup platform: separate administrative accounts outside the production domain, MFA, encryption with separately held keys, network restrictions and logging.
6. Create the isolated copy using immutable storage, a separate cloud account, offline rotated media or a vault service, with versioning to keep multiple restore points.
7. Run quarterly restore tests on a rolling sample, record timings and business sign-off, and fix what fails.
8. Exercise a ransomware scenario at least once a year in which the production domain and primary backup server are treated as lost, proving recovery from the isolated copy.
9. Report backup success rates, test results and RTO achievement to management, and feed lessons into the process review.

K Tools and Automation

- Enterprise backup and recovery platform: schedules, catalogues, encrypts and restores data across servers, virtual machines, databases and endpoints.
- SaaS backup service: protects email, collaboration and CRM data beyond the provider's native retention.
- Immutable or object-lock storage, on-premises or in the cloud: prevents deletion or alteration of backups for a defined retention period.
- Offline media (tape or removable disk rotated off-site): a low-cost, truly air-gapped option for smaller firms and for OT.
- Configuration backup tools for network devices and infrastructure-as-code repositories: allow network and cloud configuration to be rebuilt.
- Backup integrity and malware scanning before restore: helps avoid reintroducing dormant ransomware or corrupted data.
- Monitoring and ticketing integration: turns failed jobs and stale restore points into tracked actions.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
Business and data owners	Agree RTO and RPO, confirm restored data is usable, accept residual risk.
Backup administrator / IT operations	Runs and monitors backup jobs, maintains the isolated copy, performs restore tests.
CISO / information security manager	Owns backup security requirements, approves the recovery process, checks isolation and access controls.
Business continuity or risk manager	Aligns data recovery with continuity and disaster recovery plans and drills.
Data Protection Officer or privacy lead	Ensures backup retention and erasure respect personal data obligations.
MSP or cloud provider	Delivers contracted backup services and reports success rates and test results.

M Documentation and Records

- Data recovery process document (scope, priorities, RTO/RPO, security, isolation, roles, review).
- Recovery scope register with owners and objectives.
- Backup job configuration and schedule record.
- Backup security standard: encryption, key management, access and logging.
- Isolated-copy design and media rotation or retention-lock record.
- Restore test plan, test reports and ransomware exercise reports.
- Annual review record and change log.

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 17-2. Assessment testing procedures, Control 11

Test ID	Method	Testing procedure	Result
TP-C11-01	EXAMINE	11.1: Examine the data recovery process and confirm it covers scope, restoration priority, RTO and RPO, the security of backup data and the isolated copy, and that it has been approved and reviewed within the last 12 months or after the most recent significant enterprise change.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-02	INTERVIEW	11.1: Interview two business owners of critical systems to confirm they agreed the RTO and RPO recorded for their systems and know the restoration order.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-03	RE-PERFORM	11.2: Re-perform a reconciliation of the recovery scope register, the asset inventory and the backup job list, and identify any in-scope system, SaaS tenant or database with no automated job.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-04	SAMPLE	11.2: Select a sample of in-scope systems and, for several weeks spread across the review period, confirm from backup reports that a successful backup ran at least weekly, or at the higher frequency the RPO requires, and that each failure has a ticket and resolution.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-05	INSPECT	11.3: Inspect backup encryption settings for data at rest and in transit, and confirm encryption keys are held separately from the backups with a documented recovery route.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-06	INSPECT	11.3: Inspect the access list for the backup console and storage, confirm accounts are named, separate from production domain administrator accounts and protected by MFA, and review access logs for a sample period.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-07	INSPECT	11.4: Inspect the configuration of the isolated copy (retention lock, separate account or tenancy, offline rotation log) and confirm multiple restore points exist covering the defined retention period.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-08	OBSERVE	11.4: Observe an administrator attempt, using a production administrator account, to delete or alter a restore point in the isolated copy, and confirm the attempt fails. Where this is not safe to perform, examine the most recent recorded isolation test.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-09	EXAMINE	11.5: Examine the restore test plan and reports for each quarter in the review period, and confirm tests occurred at least quarterly, covered a sample of in-scope assets and recorded timings against RTO and RPO.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-10	SAMPLE	11.5: For a sample of restore tests, confirm the business owner signed off usability, failures were remediated and retested, and at least one test in the year restored from the isolated copy.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-11	OBSERVE	11.5: Select one in-scope system or data set on the day and observe the team restore it into a test environment, timing the restore and checking completeness with the data owner.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C11-12	INTERVIEW	11.5: Interview the backup administrator and CISO about the most recent ransomware recovery exercise: what was assumed lost, what was recovered from where, how long it took and what changed afterwards.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Sampling Guidance

Draw the backup sample from the recovery scope register, weighted towards critical systems and including at least one SaaS tenant, one database, one file store and, where present, one OT or network configuration item. For operating effectiveness, test backup success for four to six weeks spread across the review period, not only the weeks before the audit. Small estates (under 20 in-scope systems) can be tested in full; larger ones typically need 10 to 15 systems. For 11.5, review every quarterly test in the period and re-examine at least two in depth. A live restore on the assessment day is the strongest single piece of evidence and should be attempted where it is safe.

P Interview Questions

Interviewee	Question
Backup administrator	If the domain administrator account were compromised tonight, which backups could the attacker delete, and which could they not?
Backup administrator	When did a backup job last fail, how did you find out and how long did the fix take?
Business owner	How long could your team operate without this system, and how much data could you afford to re-enter?
CISO	Where are the backup encryption keys, and could you recover them if the primary data centre were lost?
IT manager or MSP	Which SaaS services hold enterprise data, and how is that data backed up outside the provider?
Privacy lead	How are erasure obligations for personal data handled in backup copies?

Q Technical and Process Verification

- Recovery process current, approved and aligned to agreed RTO and RPO.
- All in-scope systems, including SaaS and OT, have automated backups at the required frequency, with failures resolved.
- Backups encrypted, keys held separately, access restricted to separate MFA-protected accounts.
- An isolated, versioned copy exists that production credentials cannot alter.
- Quarterly restore tests completed with timings and business sign-off, including one from the isolated copy.

R Expected Evidence

- Data recovery process and recovery scope register.
- Backup job list reconciled to the asset inventory.
- Backup success reports and failure tickets across the period.
- Encryption and key management configuration.
- Backup platform access list, MFA configuration and access logs.
- Isolated-copy configuration and isolation test record.
- Quarterly restore test reports with business sign-off.
- Ransomware recovery exercise report and actions.

S Evaluation Criteria

Implemented

- A current recovery process with agreed objectives covers every in-scope system, and automated backups run at the required frequency with failures resolved.
- Backups are protected at least as well as the source, and an isolated, versioned copy exists outside the reach of production credentials.
- For IG2 and above, quarterly restore tests prove recoverability within objectives, including from the isolated copy.

Partially implemented

- Backups run but scope is incomplete (for example SaaS or cloud workloads omitted) or failures go unresolved.
- An off-site copy exists but shares credentials with production or has no versioning.
- Restores are tested irregularly or without timing against objectives.

Not implemented

- No documented recovery process, or backups depend on manual action.
- All backup copies are reachable and deletable from the production environment.
- No restore has been tested in the past year.

T Common Gaps and Findings

- Condition: the backup server is joined to the production domain and the backup repository is a network share. Criteria: 11.4 requires an isolated instance of recovery data. Effect: a ransomware operator with domain administrator rights can delete all backups before encrypting.
- Condition: email and collaboration data in SaaS are not backed up outside the provider's default retention. Criteria: 11.2 requires automated backups of in-scope assets. Effect: deleted or maliciously purged mailboxes cannot be recovered after the retention window.

- Condition: backup encryption keys are stored on the backup server itself. Criteria: 11.3 requires protection equivalent to the source data, and 11.1 requires backup security in the process. Effect: loss of the server makes backups unreadable, or theft exposes both data and keys.
- Condition: no restore has been attempted for the core ERP in 18 months. Criteria: 11.5 requires quarterly testing of a sample. Effect: the enterprise cannot show it can meet its RTO, and hidden failures remain undiscovered.
- Condition: the recovery process lists systems decommissioned two years ago and omits the new cloud platform. Criteria: 11.1 requires annual review and update after significant change. Effect: recovery priorities are wrong when an incident occurs.

U Remediation Guidance

- Move backup administration to accounts outside the production directory with MFA, and add immutable or offline storage with versioning for at least one copy.
- Add a SaaS backup service covering mail, collaboration and other business-critical SaaS data.
- Move encryption keys to a key management service or a sealed off-site record with documented dual-control recovery.
- Introduce a rolling quarterly restore calendar covering every critical system yearly, with timed results and owner sign-off.
- Refresh the recovery scope register from the current asset inventory, re-approve the process and add change triggers to the change management procedure.
- Run an annual ransomware recovery exercise and report the outcome to management.

V Monitoring Metrics

- Backup job success rate over the period (target 98% or higher), with mean time to resolve failures.
- Percentage of in-scope systems with a successful backup within their RPO on any given day.
- Percentage of critical systems restore-tested in the last 12 months (target 100%).
- Achieved restore time as a percentage of RTO in the latest tests.
- Percentage of in-scope data with a current isolated, immutable or offline copy.

W Related Controls and Maturity Indicators

- Control 1 and Control 3 (inventories define what must be recoverable)
- Control 3, especially 3.11 (encryption of sensitive data at rest)
- Control 5 and Control 6 (separate, MFA-protected administrative accounts for backup systems)
- Control 10 (malware defences reduce, but do not remove, the need to recover)
- Control 12 (network configuration backups and segmentation of backup infrastructure)
- Control 15 (MSP and cloud provider backup responsibilities)
- Control 17 (incident response and ransomware recovery playbooks)

Initial	Defined	Managed	Optimised
Backups exist on some systems, often manually triggered, kept on the same network; restores are attempted only when something is lost.	A documented recovery process with RTO and RPO covers in-scope systems; automated backups and an isolated copy are in place; backup access is restricted.	Backup success, coverage and restore results are measured against targets; quarterly tests prove recovery within objectives; failures are tracked to closure.	Recovery is exercised against realistic ransomware scenarios, backups are integrity-checked before restore, recovery is automated where possible and objectives are refined from test and incident data.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A Hyderabad hospital chain with five sites ran nightly backups of its hospital information system, laboratory system and radiology image store to a large disk array in its main data centre. The backup server was a member of the main domain, and a copy was replicated each night to a second array at another hospital over the same network. On paper the arrangements looked sound.

A tabletop exercise run by the new CISO asked one question: what happens if an attacker obtains domain administrator rights? The honest answer was that the same credentials could reach both arrays and delete every restore point. The exercise also showed that no one had restored the radiology store in over a year, that the laboratory system's RTO had never been agreed with clinicians, and that encryption keys for backups lived in a spreadsheet on a file server.

Over four months the hospital rewrote its data recovery process with RTO and RPO signed by the medical director, starting with identity and network services in the restoration order. Backup administration moved to separate accounts outside the domain with hardware-token MFA. A third copy was added in immutable cloud object storage under a separate account, with a 30-day retention lock and daily versioning; keys moved to a managed key service with documented break-glass recovery. Quarterly restore tests began, each timed and signed off by the system owner, and the first radiology test took 31 hours against a 12-hour RTO, which led to a change in backup design.

In the following year a ransomware attack encrypted the billing servers at one site. The production backups at that site were also hit, but the immutable copy was intact. Billing was restored within the agreed time, the incident was reported to CERT-In within the required window, and the post-incident review recorded Control 11 as the reason the outage lasted hours rather than weeks.

WP-C11: use the workpaper format shown in Appendix H.

CHAPTER 18 · CIS CONTROL 12

Network Infrastructure Management

CIS CONTROL 12 · 8 SAFEGUARDS · 1 IN IG1

Network Infrastructure Management

CIS Controls v8.1 · titles quoted verbatim | WP-C12

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 12 — Network Infrastructure Management

Control 12 deals with the network devices and design that carry everything else: routers, switches, firewalls, wireless, VPN gateways and the cloud networking constructs that now do the same jobs. It asks the enterprise to keep that infrastructure on supported, current software, to design the network in zones with only the necessary paths between them, to manage devices through controlled and encrypted means with configurations under version control, to keep accurate architecture documentation, to centralise who can log into network devices and record what they do, to use strong authentication protocols for network access, to force remote users through enterprise-managed secure access and, at IG3, to perform administration only from dedicated, segregated machines. Control 12 is about building and running the network securely; Control 13 complements it by monitoring traffic and defending against attacks in progress.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 18-1. Safeguards of CIS Control 12, Network Infrastructure Management

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
12.1	**“Ensure Network Infrastructure is Up-to-Date”**	Network	Protect	IG1	Routers, switches, firewalls, wireless controllers, VPN concentrators and similar devices run firmware or software that the maker still supports and that carries current security fixes, or are delivered as a supported network-as-a-service. Versions are checked against vendor support status at least monthly.
12.2	**“Establish and Maintain a Secure Network Architecture”**	Network	Protect	IG2	The enterprise designs its network deliberately so that systems are grouped into zones by trust and function, traffic between zones is allowed only where needed, and critical services remain available if a component fails. The design is documented and kept current.
12.3	**“Securely Manage Network Infrastructure”**	Network	Protect	IG2	Changes to and administration of network devices are carried out in a controlled, traceable and secure way: configurations are held under version control (ideally as code), administration uses encrypted protocols, and changes pass through change management.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
12.4	**“Establish and Maintain Architecture Diagram(s)”**	Documentation	Govern	IG2	Current diagrams or equivalent documentation show how the network is built: zones, key devices, links, internet and cloud connections, remote access paths and data flows. The documentation is reviewed at least yearly and after significant change.
12.5	**“Centralize Network Authentication, Authorization, and Auditing (AAA)”**	Network	Protect	IG2	Logins to network devices and network access decisions are handled by a central service that authenticates individuals, decides what each may do and records what they did, rather than relying on shared local accounts on each device.
12.6	**“Use of Secure Network Management and Communication Protocols”**	Network	Protect	IG2	Devices joining and being managed on the network use protocols that authenticate and encrypt properly: port-based network access control such as 802.1X on wired and wireless networks, WPA2-Enterprise or WPA3 for Wi-Fi, and encrypted, authenticated management traffic.
12.7	**“Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise’s AAA Infrastructure”**	Devices	Protect	IG2	Staff working on enterprise-managed devices away from the office must authenticate to the enterprise's managed VPN or equivalent secure-access service, backed by the central identity and authentication service, before they can reach internal resources.
12.8	**“Establish and Maintain Dedicated Computing Resources for All Administrative Work”**	Devices	Protect	IG3	Administrative work is done from dedicated workstations or virtual environments, physically or logically separate from the systems used for email and web browsing, placed in a segregated management network and denied general internet access.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
12.1	**1.** Maintain an inventory of network devices with model, firmware version, end-of-sale and end-of-support dates, linked to the Control 1 asset inventory. **2.** Each month, compare installed versions against the vendor's current stable releases and security advisories, and raise change tickets for devices that need upgrading. **3.** Plan replacement of hardware approaching end of support at least one budget cycle ahead. **4.** Prioritise internet-facing devices such as firewalls and VPN gateways, which are frequent targets for exploitation of known flaws.	• Network device inventory with firmware versions and support dates. • Monthly version review records and resulting change tickets. • Replacement plan for devices nearing end of support.

Safeguard	Practical steps	Evidence
12.2	**1.** Define zones (for example user, server, management, guest, DMZ, OT, payment or personal-data zones) and the permitted flows between them, on a default-deny basis. **2.** Apply least privilege to network paths: each flow should have a business owner and a reason, recorded in a rule base or flow matrix. **3.** Design for availability, with redundant links, devices or providers for services the business cannot do without. **4.** Record the architecture in policy and design documents and review it when major changes occur.	• Network architecture or security design document describing zones, permitted flows and resilience. • Firewall rule base or flow matrix with owners and justifications. • Evidence of redundancy for critical network services.
12.3	**1.** Store device configurations in a version-controlled repository, either as infrastructure-as-code or as automatic configuration backups, so that every change can be compared and rolled back. **2.** Disable cleartext management protocols (Telnet, HTTP, older SNMP versions) and use SSH, HTTPS or other encrypted alternatives. **3.** Require all network changes to go through change management with approval and post-change verification. **4.** Compare running configurations against the approved baseline regularly and investigate unexplained differences.	• Configuration repository or backup tool showing version history for network devices. • Device configurations showing management restricted to encrypted protocols. • Change records for a sample of network changes, and drift reports.
12.4	**1.** Produce a logical diagram (zones, security boundaries, flows) and, for larger networks, a physical diagram (sites, links, devices). **2.** Include cloud networks, SaaS connectivity, third-party links and remote access, which are often missing from older diagrams. **3.** Assign an owner, keep diagrams under version control and review them yearly and after major projects. **4.** Classify the diagrams as restricted, since they are valuable to an attacker.	• Current logical and physical network diagrams with version and review date. • Review records showing updates after significant changes. • Access restrictions on the diagram repository.
12.5	**1.** Deploy a central AAA service (for example RADIUS or TACACS+ linked to the enterprise directory) for administrative access to network devices. **2.** Give each administrator an individual account with role-based command authorisation, and protect administrative access with MFA where the platform allows. **3.** Keep a single local break-glass account per device, with its credential vaulted and its use alerted. **4.** Send accounting records to the central log platform and review them.	• AAA server configuration and device configurations pointing to it. • List of administrators and roles, and break-glass account controls. • Sample accounting logs showing individual attribution of device changes.

Safeguard	Practical steps	Evidence
12.6	**1.** Configure corporate Wi-Fi with WPA2-Enterprise or WPA3-Enterprise using certificate-based or directory-backed authentication, and separate guest Wi-Fi from internal networks. **2.** Roll out 802.1X or an equivalent network access control on wired ports in offices, with a fallback quarantine network for devices that fail. **3.** Use SNMPv3 with authentication and encryption, and secure versions of other management and time protocols. **4.** Retire pre-shared Wi-Fi keys and legacy protocols on a dated plan.	• Wireless controller configuration showing enterprise authentication. • Network access control configuration and a sample of authentication logs. • Device configurations showing secure management protocol versions.
12.7	**1.** Provide an enterprise-managed VPN or zero-trust network access service and route access to internal resources through it. **2.** Authenticate users against the enterprise directory with MFA, and check device posture (managed, patched, protected) before granting access. **3.** Block direct exposure of internal services such as remote desktop to the internet. **4.** Log remote access sessions centrally and review unusual connections.	• VPN or secure-access configuration showing directory integration and MFA. • Device posture policy and evidence of enforcement. • Remote access logs for a sample period and external scan showing no exposed internal services.
12.8	**1.** Provide privileged access workstations (physical or hardened virtual machines) for administrators of the directory, network, cloud consoles and critical servers. **2.** Place them in a management zone that alone can reach device and server management interfaces, and block their internet access except to explicitly approved update or cloud-administration endpoints. **3.** Prohibit email, general browsing and personal use on these workstations, and harden them beyond the standard baseline. **4.** Restrict administrative interfaces so they accept connections only from the management zone.	• Inventory and configuration of administrative workstations. • Firewall rules showing management interfaces reachable only from the management zone, and blocked internet access. • Policy prohibiting general use of administrative workstations.

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
IG1 has one Safeguard in this Control: keep network infrastructure up to date (12.1), with a monthly look at versions and support status. For a 40-person firm this means knowing which router, firewall and Wi-Fi access points it has, confirming they are still supported, applying updates or using a managed service that does, and replacing devices that have reached end of life.	IG2 adds most of the Control: a secure network architecture with segmentation, least privilege and availability (12.2), secure management with version-controlled configurations and encrypted protocols (12.3), maintained architecture diagrams (12.4), centralised AAA for network devices (12.5), secure network access and management protocols such as 802.1X and enterprise Wi-Fi (12.6) and enterprise-managed VPN with central authentication for remote devices (12.7). Together these turn the network from a set of boxes into a governed, documented and controlled system.	IG3 adds dedicated computing resources for all administrative work (12.8): privileged access workstations in a segregated management network without general internet access. This protects the enterprise against attackers who target administrators specifically, which is common in sophisticated intrusions.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 12.1 → 8.8 Management of technical vulnerabilities; 8.20 Networks security; 7.13 Equipment maintenance
- 12.2 → 8.20 Networks security; 8.22 Segregation of networks; 8.14 Redundancy of information processing facilities; 8.27 Secure system architecture and engineering principles
- 12.3 → 8.9 Configuration management; 8.32 Change management; 8.20 Networks security
- 12.4 → 8.20 Networks security; 5.9 Inventory of information and other associated assets; 5.37 Documented operating procedures
- 12.5 → 8.5 Secure authentication; 5.15 Access control; 8.2 Privileged access rights; 8.15 Logging
- 12.6 → 8.20 Networks security; 8.21 Security of network services; 8.5 Secure authentication
- 12.7 → 6.7 Remote working; 8.1 User endpoint devices; 8.5 Secure authentication; 8.20 Networks security
- 12.8 → 8.2 Privileged access rights; 8.22 Segregation of networks; 8.18 Use of privileged utility programs (supporting)

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: PR.IR-01 (networks and environments protected from unauthorised logical access); PR.PS-01 (configuration management); PR.PS-02 (software maintained); PR.AA-05 (access permissions and least privilege); ID.AM-03 (representations of network communication and data flows maintained) — Srida IT mapping
- NIST SP 800-53 Rev. 5: SC-7 Boundary Protection; AC-17 Remote Access; IA-3 Device Identification and Authentication; CM-2 and CM-3 Baseline Configuration and Change Control; SI-2 Flaw Remediation
- IEC 62443-3-3: zones and conduits model for OT network segmentation, relevant to 12.2 in industrial settings
- CIS Benchmarks for network device platforms: secure configuration references for 12.3 and 12.6 for current availability

F India Regulatory Touchpoints

- CERT-In Directions of 28 April 2022: clock synchronisation to NTP servers of NIC or NPL (or traceable sources), and 180-day retention of logs including network device logs; well-managed network infrastructure is the practical basis for both.
- RBI cyber security framework and IT governance directions: network segmentation, secure remote access with MFA and controlled administration of network devices for banks and NBFCs.
- SEBI CSCRF (2024): network segmentation, secure remote access and privileged access management expectations for regulated entities.
- CERT-In empanelled security audits: network architecture and device configuration reviews are typical audit scope items for regulated and government-linked entities.

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Network devices are high-value targets. Firewalls and VPN gateways sit on the internet edge, often run old firmware, rarely have endpoint protection and frequently have known exploitable flaws that attackers scan for within days of disclosure. A compromised edge device gives the attacker a foothold with visibility of traffic and a path inward. Inside the network, a flat design lets a single infected laptop reach every server, backup system and plant controller; segmentation is what keeps a contained incident from becoming an enterprise-wide one.

The administrative side matters as much as the technical design. Shared local passwords on switches, Telnet still enabled, changes made directly on devices without records, and administrators reading email on the same laptop they use to manage the core firewall: each of these lets an attacker who steals one credential or infects one machine take control of the network. Without current diagrams, incident responders lose hours working out what connects to what.

In India, CERT-In has repeatedly warned about exploitation of network edge devices, and its April 2022 Directions require enterprises to synchronise clocks to designated NTP sources and to retain logs for 180 days, both of which depend on well-managed network infrastructure. Sector regulators, including RBI and SEBI under CSCRF, expect network segmentation, secure remote access and controlled administration. Many Indian SMEs still run end-of-life routers supplied by an internet provider, with default credentials and remote management open to the internet.

I Applicability

Every enterprise has network infrastructure, even if it is a single router from the internet provider. A 40-person Kochi CA firm meets IG1 by knowing its router, firewall and access points, confirming firmware support, enabling automatic updates or arranging them through its IT provider, and changing default administrative credentials; it should also take the practical IG2 steps of separating guest Wi-Fi and disabling remote management from the internet. Cloud and SaaS-heavy enterprises still own their cloud network design (virtual networks, security groups, private endpoints), secure access for staff and infrastructure-as-code for cloud networking; their Control 12 lives largely in the cloud console and code repository. OT environments, such as a Chennai auto-parts plant, need strong segmentation between IT and OT, a controlled DMZ for data exchange, and careful update planning because plant network devices may need maintenance windows. Where an MSP or telecom provider manages the network, the enterprise must still obtain version reports, configuration backups, change records and AAA logs, and ensure that the provider's own administrative access is individual, MFA-protected and logged.

J Implementation Guidance

1. Build the network device inventory with versions and support dates, and start the monthly version and advisory review, fixing internet-facing devices first.
2. Document the current architecture and draw logical and physical diagrams, including cloud, third-party and remote access paths.
3. Design the target architecture: zones, permitted flows on a default-deny basis, resilience for critical services and a management zone.
4. Implement segmentation in stages, starting with the highest-value separations: guest from internal, users from servers, IT from OT, backup and management networks from everything else.
5. Centralise administrative access through an AAA service with individual accounts, role-based authorisation, MFA and vaulted break-glass credentials.
6. Move configurations into version control or automatic configuration backup, disable cleartext management protocols and put all network changes through change management.
7. Introduce enterprise Wi-Fi authentication and wired network access control, retiring shared Wi-Fi keys.
8. Route remote access through an enterprise-managed VPN or zero-trust service with directory authentication, MFA and device posture checks, and close any directly exposed internal services.
9. For IG3, provide privileged access workstations in the management zone, restrict management interfaces to that zone and block general internet access from it.
0. Review the architecture and diagrams at least yearly and after major change, and feed network device logs to central logging (Control 8) and monitoring (Control 13).

K Tools and Automation

- Network configuration management and backup tools: capture, version and compare device configurations, detect drift and support rollback.
- Infrastructure-as-code tooling and a version-controlled repository: define cloud and on-premises network configuration as reviewed code.
- AAA services (RADIUS, TACACS+) integrated with the enterprise directory: central authentication, command authorisation and accounting for network devices.
- Network access control (NAC) and enterprise wireless controllers: enforce 802.1X and device-based admission to wired and wireless networks.
- VPN or zero-trust network access platforms with posture checking: provide controlled remote access to internal resources.
- Vulnerability scanners (for example OpenVAS/Greenbone) and external attack surface scanning: identify outdated firmware and exposed management interfaces.
- Network diagramming and documentation tools, ideally linked to discovery data: keep diagrams current.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
Network team / network engineer	Maintains devices, configurations, segmentation, AAA, NAC and VPN; carries out approved changes.
Security architect or CISO	Owns the secure network architecture, approves zone and flow design, accepts exceptions.
Change advisory board or change manager	Approves and reviews network changes.
Privileged administrators	Use individual accounts and dedicated administrative workstations; follow change procedures.
OT / plant engineering lead	Agrees OT segmentation, maintenance windows and data-exchange design.
MSP or telecom provider	Manages contracted devices, supplies version reports, configuration backups and access logs.

M Documentation and Records

- Network security standard covering zones, permitted flows, secure protocols, AAA and remote access.
- Network device inventory with versions and support dates.
- Logical and physical network diagrams with version control and review dates.
- Firewall rule base or flow matrix with owners and justifications.
- Configuration repository, baseline configurations and change records.
- Remote access standard and privileged access workstation standard.
- Monthly version review records and annual architecture review records.

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 18-2. Assessment testing procedures, Control 12

Test ID	Method	Testing procedure	Result
TP-C12-01	**RE-PERFORM**	12.1: Re-perform a comparison of installed firmware or software versions on all network devices (or a sample for large estates) against vendor support status and security advisories, and list devices that are unsupported or missing security releases.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-02	**SAMPLE**	12.1: Select several months across the review period and confirm that the version review took place at least monthly, and that resulting upgrades were ticketed and completed or formally risk-accepted.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-03	**EXAMINE**	12.2: Examine the network architecture document and confirm it defines zones, permitted flows on a default-deny basis and resilience arrangements for critical services.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-04	**SAMPLE**	12.2: Select a sample of firewall or security-group rules, including any broad 'any-any' rules, and confirm each has an owner, a business justification and a recent review. From a user-zone host, attempt connections to server, management and OT zones and confirm only permitted flows succeed.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-05	**INSPECT**	12.3: Inspect the configuration repository or backup tool for a sample of devices to confirm version history exists, and inspect device configurations to confirm Telnet, HTTP management and insecure SNMP versions are disabled.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-06	**SAMPLE**	12.3: Select a sample of configuration changes from the repository history across the period and trace each to an approved change record; investigate any change without one.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C12-07	**EXAMINE**	12.4: Examine the network diagrams and compare them with the device inventory, the firewall rule base and cloud network configuration, noting any missing zones, links, cloud connections or third-party paths. Confirm the last review date is within 12 months and after the latest significant change.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-08	**INSPECT**	12.5: Inspect the AAA configuration and a sample of device configurations to confirm administrative login uses central authentication, that roles restrict commands and that a single vaulted break-glass account is the only local account.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-09	**SAMPLE**	12.5: Select a sample of device changes and confirm accounting logs attribute each to an individual administrator; check whether any break-glass use was alerted and justified.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-10	**INSPECT**	12.6: Inspect wireless controller settings for WPA2-Enterprise or WPA3-Enterprise on corporate networks and separation of guest Wi-Fi, and inspect wired network access control settings and authentication logs.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-11	**OBSERVE**	12.6: Observe the connection of an unmanaged device to a wired office port and to corporate Wi-Fi and confirm it is refused or placed in a quarantine network.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-12	**INSPECT**	12.7: Inspect VPN or secure-access configuration to confirm directory authentication, MFA and device posture checks, and review an external scan to confirm no internal services such as remote desktop are directly exposed to the internet.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-13	**SAMPLE**	12.7: Select a sample of remote users and confirm from access logs over the period that their access to internal resources passed through the enterprise-managed VPN or secure-access service.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-14	**INSPECT**	12.8: Inspect the inventory and configuration of administrative workstations, and confirm they sit in a management zone, are blocked from general internet access and are the only sources allowed to reach management interfaces.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C12-15	**INTERVIEW**	12.8: Interview a sample of administrators about where they carry out administrative tasks and how they read email, and confirm by observation that administrative consoles cannot be reached from a standard user workstation.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

For small networks (under 20 network devices), review every device. For larger estates, sample by type and role so that firewalls, edge VPN gateways, core switches, wireless controllers and cloud network constructs are all represented, always including every internet-facing device. For changes and accounting logs, sample across the whole review period, typically 10 to 25 changes depending on volume, including emergency changes. Firewall rule samples should be risk-weighted towards broad rules, rules to sensitive zones and rules with no recent review. For remote access, sample users from different roles, including administrators and third parties.

P Interview Questions

Interviewee	Question
Network engineer	Which network devices are past or close to end of support, and what is the plan for each?
Network engineer	If I changed a switch configuration directly on the device tonight, how and when would anyone know?
Security architect	Which zones can reach the backup and management networks, and why?
Privileged administrator	From which machine do you log into the core firewall, and do you use that machine for email?

Interviewee	Question
IT manager or MSP	How do your engineers authenticate to our devices, and can we see their access logs?
OT lead	What paths exist between the office network and the plant network, and who approves new ones?

Q Technical and Process Verification

- All network devices are on supported software, with monthly reviews and timely upgrades.
- The network is segmented according to a documented architecture, with justified rules and tested isolation.
- Configurations are version-controlled, managed over encrypted protocols and changed only through change management.
- Diagrams are current and complete, including cloud and remote access.
- Network administration uses central AAA with individual attribution, and network access uses strong protocols.
- Remote access is via an enterprise-managed service with MFA, and (IG3) administration is done from dedicated, segregated workstations.

R Expected Evidence

- Network device inventory with versions and support status.
- Monthly version review records and upgrade tickets.
- Network architecture document, flow matrix and firewall rule review.
- Configuration repository history and change records.
- Current logical and physical diagrams with review dates.
- AAA configuration and accounting logs.
- Wireless and NAC configuration with authentication logs.
- VPN or secure-access configuration, logs and external exposure scan.
- Administrative workstation configuration and management zone rules.

S Evaluation Criteria

Implemented

- All network devices are supported and reviewed monthly, with upgrades completed or formally accepted.
- For IG2, the network follows a documented segmented design, devices are managed securely through central AAA with version-controlled configurations, diagrams are current, network access uses strong protocols and remote access goes through an enterprise-managed service with MFA.
- For IG3, administration is done only from dedicated workstations in a segregated management network without internet access.

Partially implemented

- Most devices are supported but internet-facing devices lag on security releases, or reviews are irregular.
- Segmentation exists but broad rules undermine it, or diagrams omit cloud and third-party connections.
- Central AAA is in place for some devices while others still use shared local accounts.

Not implemented

- Network devices run unsupported firmware with no review process.
- The network is flat, with no defined zones or flow control.
- Remote access relies on directly exposed services or shared credentials without MFA.

T Common Gaps and Findings

- Condition: the edge VPN gateway runs firmware with a publicly known critical flaw, unpatched for four months. Criteria: 12.1 requires current, supported network software reviewed monthly. Effect: an attacker can gain remote access to the internal network without credentials.
- Condition: user, server, backup and OT systems share one flat network. Criteria: 12.2 requires segmentation and least privilege in the network architecture. Effect: one infected laptop can reach every critical system, including backups.
- Condition: all switches share one local administrator password known to the MSP's whole team. Criteria: 12.5 requires centralised AAA. Effect: changes cannot be attributed and a single leaked password exposes the whole network.

- Condition: network diagrams date from before the cloud migration. Criteria: 12.4 requires review annually and after significant change. Effect: responders and auditors cannot see the actual attack surface.
- Condition: remote desktop is exposed directly to the internet for staff working from home. Criteria: 12.7 requires remote access through an enterprise-managed VPN with central authentication. Effect: password-guessing and exploitation of remote desktop give attackers a direct entry route.
- Condition: administrators manage the core firewall from their everyday laptop. Criteria: 12.8 (IG3) requires dedicated administrative resources. Effect: a phishing compromise of one administrator yields control of the network.

U Remediation Guidance

- Patch or replace vulnerable and end-of-support edge devices immediately, then start a documented monthly version review.
- Design and implement segmentation in stages, starting with backup, management and OT separation, enforced on a default-deny basis.
- Deploy central AAA with individual accounts and MFA, vault a single break-glass credential per device and require the MSP to use individual accounts.
- Redraw the network diagrams to include cloud, third-party and remote access paths, and add diagram updates to the change process.
- Close directly exposed remote desktop and route all remote access through an enterprise-managed VPN or zero-trust service with MFA and posture checks.
- Provide privileged access workstations and restrict management interfaces to the management zone.

V Monitoring Metrics

- Percentage of network devices on supported software with current security releases (target 100% for internet-facing devices).
- Median days from vendor security advisory to deployment on affected network devices.
- Percentage of firewall rules with an owner and a review in the last 12 months.
- Percentage of network device logins via central AAA with individual accounts.
- Number of internal services directly exposed to the internet (target zero).

W Related Controls and Maturity Indicators

- Control 1 (network devices in the asset inventory)
- Control 4, especially 4.2 (secure configuration of network infrastructure)
- Control 5 and Control 6 (administrative accounts, MFA and privileged access)
- Control 7 (vulnerability management for network devices)
- Control 8 (network device logs and time synchronisation)
- Control 11 (backup of network configurations; isolation of backup networks)
- Control 13 (network monitoring and defence)
- Control 15 (MSP and telecom provider oversight)

Initial	Defined	Managed	Optimised
Network devices are installed and left alone; firmware is rarely updated, the network is largely flat, administration uses shared local accounts and diagrams are out of date.	A network security standard and current diagrams exist; devices are inventoried and reviewed monthly; segmentation and central AAA are designed and partly implemented.	Segmentation, AAA, secure protocols, enterprise Wi-Fi and managed remote access are fully in place; configuration changes are version-controlled and traced to change records; metrics are reported.	Network configuration is defined as code with automated testing and drift detection; segmentation is refined from monitoring and threat intelligence; administration is done only from dedicated workstations; zero-trust access replaces broad network trust.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A Bengaluru SaaS start-up with 180 staff ran its product entirely in the cloud, and its founders assumed Control 12 did not really apply. A customer security questionnaire from a large Indian bank suggested otherwise. The review that followed found a small office network with an end-of-support firewall supplied years earlier, Wi-Fi protected by a shared password printed on the wall, and engineers connecting to cloud databases over public endpoints restricted only by their home IP addresses, which changed often and were added to security groups by hand.

The head of security set out a 90-day plan. The office firewall was replaced with a supported model and added to a monthly version review alongside the cloud provider's managed network services. Office Wi-Fi moved to WPA3-Enterprise using directory credentials, with a separate guest network. In the cloud, the team defined virtual networks, subnets and security groups as infrastructure-as-code in a version-controlled repository, so every change went through pull-request review and could be rolled back. Production, staging and corporate tooling were placed in separate networks with flows only where justified, and database endpoints were made private.

Public database access was removed and engineers now reached production through an enterprise-managed zero-trust access service tied to the directory, requiring MFA and a managed, encrypted laptop. Logical diagrams were generated from the code repository and reviewed at each quarterly architecture meeting. For the few engineers with full production rights, the company provided hardened cloud workstations with no general internet access, the only sources allowed to reach the cloud administrative consoles.

The bank's assessor rated the start-up's network controls acceptable. The CTO noted that the infrastructure-as-code history also answered the auditor's change management questions, with every network change traceable to a reviewed and approved request.

WP-C12: use the workpaper format shown in Appendix H.

CHAPTER 19 · CIS CONTROL 13

Network Monitoring and Defense

CIS CONTROL 13 · 11 SAFEGUARDS · 0 IN IG1

Network Monitoring and Defense

CIS Controls v8.1 · titles quoted verbatim | WP-C13

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 13 — Network Monitoring and Defense

Control 13 is about seeing and controlling what happens on the network, and about having people and processes that act on what is seen. It moves an enterprise from preventive hygiene, such as patching, configuration and access control, to an operating capability: events collected in one place and correlated, sensors on hosts and at network chokepoints, filtering between zones and at the application layer, posture checks for remote devices, flow records that show who talked to whom, and alert rules that are tuned rather than left to drift. Every one of its eleven Safeguards sits at IG2 or IG3. That does not mean a small firm can ignore network defence; it means CIS expects the foundations from Controls 1 to 12 (inventories, secure configuration, logging, malware defence and network infrastructure management) to be in place first, because a monitoring programme built on an unknown estate produces noise rather than assurance. The Control has a strong human element. Tools that alert into an unread mailbox satisfy nobody, so an assessor looks as much for triage records, response targets and monthly tuning as for the presence of a SIEM or an IDS.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 19-1. Safeguards of CIS Control 13, Network Monitoring and Defense

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
13.1	**“Centralize Security Event Alerting”**	Network	Detect	IG2	Security-relevant events from servers, endpoints, network devices, identity systems and cloud services are brought into one place where correlation rules raise alerts that a named person or team actually receives and works. A SIEM is the usual answer; a log analytics platform running security correlation content is an acceptable alternative.
13.2	**“Deploy a Host-Based Intrusion Detection Solution”**	Devices	Detect	IG2	Servers and end-user devices carry an agent or built-in capability that watches the host itself, such as file integrity, registry and service changes, suspicious process behaviour and local logon activity, and reports what it sees, wherever the platform can support it.
13.3	**“Deploy a Network Intrusion Detection Solution”**	Network	Detect	IG2	Traffic crossing important points in the network, or flowing within a cloud environment, is inspected by a sensor that recognises attack signatures and abnormal patterns and raises alerts; in cloud workloads the provider's native threat detection service can play this role.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
13.4	**“Perform Traffic Filtering Between Network Segments”**	Network	Protect	IG2	Where the network is divided into zones, the boundaries between those zones enforce rules about which traffic may pass, rather than leaving internal networks flat; rules follow a default-deny stance and are justified by business need.
13.5	**“Manage Access Control for Remote Assets”**	Devices	Protect	IG2	Devices that connect from outside, such as laptops on VPN or zero-trust access, are checked for health before and during the session, and the level of access they receive depends on whether anti-malware is running and current, whether the device matches the approved configuration, and whether its operating system and applications are patched.
13.6	**“Collect Network Traffic Flow Logs”**	Network	Detect	IG2	Network devices export flow records (who talked to whom, on which port, for how long, how much data) or full packet captures at key points, and these records are retained, reviewed and used to raise alerts.
13.7	**“Deploy a Host-Based Intrusion Prevention Solution”**	Devices	Protect	IG3	Endpoints and servers run a capability that does not only report suspicious host activity but stops it, for example by killing a process, blocking an exploit or isolating the device; an EDR agent in blocking mode or a host IPS agent are typical.
13.8	**“Deploy a Network Intrusion Prevention Solution”**	Network	Protect	IG3	At selected network chokepoints, a sensor sits in line and actively drops traffic that matches attacks, rather than merely raising an alert; a cloud provider's native inline protection is an acceptable equivalent.
13.9	**“Deploy Port-Level Access Control”**	Network	Protect	IG3	A switch port or wireless network will only admit a device once it has authenticated, typically through 802.1X with certificates or credentials, so that an unknown machine plugged into a wall socket or meeting-room port does not join the corporate network.
13.10	**“Perform Application Layer Filtering”**	Network	Protect	IG3	Traffic is inspected and filtered at the application layer, not only by address and port: a filtering proxy for web traffic, a web application firewall in front of published applications, or a gateway that understands the protocol and blocks misuse.
13.11	**“Tune Security Event Alerting Thresholds”**	Network	Detect	IG3	Alert thresholds and correlation rules are reviewed and adjusted at least once a month, using what analysts learned from false positives, missed detections and changes to the environment, so that alerts stay meaningful.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
13.1	**1.** Define the log sources in scope from the asset inventory (Control 1) and the logging standard (Control 8): domain controllers, firewalls, VPN, email gateway, EDR console, cloud audit trails and critical applications at a minimum. **2.** Forward those sources to a central platform with synchronised timestamps, and confirm each source is parsed into named fields rather than stored as raw text. **3.** Enable a starter set of correlation rules (for example brute force followed by a successful logon, new administrator creation, logon from an unusual country, mass file renames) and route each alert to a queue with an owner and a response target. **4.** Monitor the health of the pipeline itself: raise an alert when a source goes silent for longer than an agreed interval.	• Log source register showing each source, its owner, its ingestion status and the date it was last seen • Correlation rule catalogue with the queue and owner each rule alerts to • Sample of alert tickets showing triage notes and closure
13.2	**1.** Choose the host detection capability per platform: the detection side of an EDR agent, an open-source host agent such as Wazuh or osquery-based monitoring, or the native auditing of the operating system feeding the SIEM. **2.** Deploy it first to internet-facing servers, domain controllers and systems holding sensitive data, then to the wider estate, and record exceptions (appliances, legacy or vendor-locked systems) with a compensating control. **3.** Feed host detections into the central alert platform from 13.1 so they are correlated with network and identity events.	• Agent coverage report reconciled against the asset inventory, with exceptions listed • Configuration or policy export showing which host events are watched • Example host alerts with their triage records
13.3	**1.** Map the chokepoints worth watching: internet edge, links between user and server zones, data-centre or cloud ingress, and the boundary with any OT or partner network. **2.** Place sensors on span ports, network taps or virtual mirrors at those chokepoints, or switch on the cloud provider's threat detection for each account or subscription; open-source engines such as Suricata or Zeek are reasonable for smaller budgets. **3.** Keep signatures and threat intelligence feeds current, and send sensor alerts to the central platform.	• Network diagram marking sensor or cloud detection placement • Signature or rule-set update history • Sample alerts generated by the sensors
13.4	**1.** Define zones from the data and asset classification: for example users, servers, management, guest, payment or patient-data systems, OT and third-party connections. **2.** Place filtering (internal firewall, ACLs on layer-3 switches, cloud security groups or micro-segmentation) between zones and write rules that allow only named flows. **3.** Review the rule base on a fixed cycle and after major changes, removing any-any rules, unused rules and expired temporary openings.	• Zone model and inter-zone flow matrix • Firewall or security group rule export with owner and justification fields • Rule review record with rules removed or tightened

Safeguard	Practical steps	Evidence
13.5	**1.** Define the posture checks: anti-malware or EDR present and updated, disk encryption on, required configuration baseline met, operating system and key applications within the patch window. **2.** Enforce the checks in the remote access path (VPN posture assessment, zero-trust network access policy or MDM-based conditional access) and decide what a failing device gets: blocked, or limited to a remediation network. **3.** Treat unmanaged personal devices as a separate case with restricted, browser-only or virtual-desktop access.	• Remote access posture policy settings • Logs of devices denied or quarantined for failing posture • Exception list for devices permitted without full posture checks, with approvals
13.6	**1.** Enable NetFlow, IPFIX, sFlow or equivalent on core switches, routers and firewalls, and enable VPC or VNet flow logs in cloud accounts. **2.** Send flow records to a collector or the SIEM, and retain them for the period required by policy and regulation. **3.** Build alerts on flow data for patterns such as unusually large outbound transfers, connections to known-bad destinations, internal scanning and traffic on unexpected ports.	• Configuration showing flow export on named devices and cloud accounts • Collector or SIEM retention settings • Flow-based alert rules and a sample of alerts raised
13.7	**1.** Move the host agent from audit-only to blocking for well-understood behaviours (credential dumping, ransomware-style encryption, known exploit techniques) after a tuning period. **2.** Define who may isolate a host and under what conditions, and test that isolation works without cutting the response team's own access. **3.** Track coverage and policy mode per asset group so that silently downgraded agents are noticed.	• EDR or host IPS policy showing prevention settings per group • Records of blocked or isolated events • Coverage report showing agent mode by asset group
13.8	**1.** Identify where inline blocking is justified by risk and where availability concerns argue for detect-only, and record the decision. **2.** Enable prevention mode for a curated rule set, starting with high-confidence signatures, and monitor for false drops during a pilot period. **3.** Agree a fail-open or fail-closed setting for each inline device with the business owner of the traffic it protects.	• IPS policy showing which signatures are set to block • Change records for moving rules into prevention mode • Log of blocked sessions with periodic review notes
13.9	**1.** Issue device certificates to managed assets through the PKI or MDM, and stand up a RADIUS-based network access control service. **2.** Enable 802.1X on corporate wireless first, then on wired access ports, with MAC authentication bypass only for documented devices such as printers or IP phones placed in restricted VLANs. **3.** Send unauthenticated devices to a guest or quarantine VLAN and alert on repeated failures.	• Switch and wireless controller configuration showing port authentication • NAC policy and the MAC-by-pass register • NAC logs showing denied or quarantined devices

Safeguard	Practical steps	Evidence
13.10	**1.** Route outbound web traffic through a proxy or secure web gateway that enforces category and reputation filtering, and decide the approach to TLS inspection with legal and privacy input. **2.** Place a web application firewall or API gateway in front of internet-facing applications, starting in monitoring mode and moving to blocking after tuning. **3.** Apply protocol-aware controls on other risky channels such as DNS filtering and email gateways where these are not already handled under Controls 9 and 12.	• Proxy, WAF or gateway policy export • Blocking statistics and sample blocked requests • TLS inspection policy and its approved exemptions
13.11	**1.** Hold a monthly tuning review that looks at alert volume per rule, false-positive rate, alerts closed without action and any incident that was missed or detected late. **2.** Change thresholds, suppressions and rule logic through change control, recording the reason for each change so that risky suppressions can be challenged. **3.** Re-test tuned rules where possible (replayed logs or simulated activity) to confirm they still fire on genuine attack behaviour.	• Monthly tuning minutes or tickets for each month in the period • Rule change log with reasons • Alert quality metrics showing trend over time

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
Control 13 has no IG1 Safeguards. An IG1 enterprise is not expected to run a SIEM or intrusion sensors, but it should not be blind either: the IG1 Safeguards elsewhere (audit log collection in 8.1 to 8.3, anti-malware in 10.1 to 10.3, firewalls on servers and end-user devices in 4.4 and 4.5, and up-to-date network infrastructure in 12.1) give it basic visibility and filtering. A 40-person firm can meet the spirit of this Control by making sure its firewall, endpoint protection console and Microsoft 365 or Google Workspace alerts go to a person who reads them, and that the CERT-In log retention expectation is met.	IG2 introduces six Safeguards that together form a basic security monitoring operation: central alerting with correlation (13.1), host-based detection (13.2), network detection at chokepoints or in the cloud (13.3), filtering between network segments (13.4), posture-based access control for remote devices (13.5) and collection of traffic flow logs (13.6). An IG2 enterprise can run this in-house with a small team or through a managed SOC or MDR provider, but it must own the decisions: what is monitored, who receives alerts and how quickly they are handled.	IG3 adds five Safeguards that turn detection into prevention and sharpen the signal: host-based prevention such as EDR in blocking mode (13.7), inline network prevention (13.8), port-level authentication such as 802.1X (13.9), application layer filtering through proxies, WAFs or gateways (13.10) and monthly tuning of alert thresholds (13.11). These are expected of enterprises handling sensitive data at scale or facing determined adversaries, and they assume the IG2 monitoring base is mature enough that blocking decisions are made on reliable signals.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 13.1 → 8.15 Logging; 8.16 Monitoring activities; 5.25 Assessment and decision on information security events
- 13.2 → 8.16 Monitoring activities; 8.7 Protection against malware; 8.1 User endpoint devices
- 13.3 → 8.16 Monitoring activities; 8.20 Networks security
- 13.4 → 8.22 Segregation of networks; 8.20 Networks security
- 13.5 → 6.7 Remote working; 8.1 User endpoint devices; 8.5 Secure authentication
- 13.6 → 8.15 Logging; 8.16 Monitoring activities
- 13.7 → 8.7 Protection against malware; 8.16 Monitoring activities
- 13.8 → 8.20 Networks security; 8.21 Security of network services
- 13.9 → 8.20 Networks security; 8.5 Secure authentication
- 13.10 → 8.23 Web filtering; 8.20 Networks security; 8.26 Application security requirements
- 13.11 → 8.16 Monitoring activities; clause 10.1 Continual improvement

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0 (Srida IT mapping): DE.CM-01 networks monitored (13.3, 13.6, 13.8); DE.CM-09 computing hardware and software monitored (13.2, 13.7); DE.AE-02 and DE.AE-03 event analysis and correlation (13.1, 13.11); PR.IR-01 networks protected from unauthorised logical access (13.4, 13.9, 13.10); PR.AA-03 authentication (13.5, 13.9)
- NIST SP 800-53 Rev. 5: SI-4 System Monitoring; AU-6 Audit Record Review, Analysis and Reporting; SC-7 Boundary Protection; AC-4 Information Flow Enforcement; AC-17 Remote Access; IA-3 Device Identification and Authentication
- MITRE ATT&CK: detection and prevention coverage under this Control is usefully expressed as ATT&CK technique coverage, for example lateral movement and exfiltration techniques

F India Regulatory Touchpoints

- CERT-In Directions of 28 April 2022 under section 70B(6) of the IT Act: reporting of specified cyber incidents within six hours of noticing them, retention of ICT system logs for 180 days within India, and synchronisation of clocks to NIC or NPL time sources. Central alerting (13.1) and flow logs (13.6) are the practical means of meeting detection and log expectations
- SEBI Cybersecurity and Cyber Resilience Framework (CSCRF, 2024): regulated entities are expected to have SOC capability (own, group or market-level) and continuous monitoring scaled to their category
- RBI cyber security and IT governance directions for banks and NBFCs: expectations of a security operations capability, network segmentation and monitoring of anomalous activity, with incident reporting to RBI on short timelines
- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6: reasonable security safeguards for personal data, which the Rules describe as including monitoring and logging of access to personal data and the ability to detect and investigate unauthorised access

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Most damaging intrusions are not single events. An attacker phishes a user, lands on a laptop, harvests credentials, moves laterally to a file server, stages data and then either exfiltrates it or deploys ransomware. Each step leaves traces on hosts and in network traffic, and each is an opportunity to stop the attack if somebody is watching. Without central alerting, host and network sensors, and flow records, those traces sit unread across dozens of devices, and the first sign of trouble is a ransom note or a call from a regulator. Flat internal networks make the problem worse because a single compromised machine can reach everything, which is why the filtering, port authentication and remote posture Safeguards matter as much as the detection ones.

The opposite failure is just as common: tools are bought, switched on with default rules, and drown a small team in alerts until the console is ignored. Untuned detection gives management a comfortable dashboard while real attacks pass unnoticed. Control 13 therefore pairs the technology with the discipline of routing alerts to owners, measuring alert quality and tuning thresholds every month, and it expects coverage to be reconciled against the asset inventory so that blind spots are known rather than discovered during an incident.

In India the business case is reinforced by regulation. The CERT-In Directions of April 2022 expect specified incidents to be reported within six hours of being noticed and expect logs to be kept for a rolling 180 days within Indian jurisdiction, with clocks synchronised to an authorised time source. An enterprise that cannot detect an incident quickly cannot report it within six hours, and one that does not keep network and security logs cannot answer CERT-In's follow-up questions. Sector regulators such as SEBI, RBI and IRDAI go further for their regulated entities, expecting security operations centre capability and continuous monitoring proportionate to the entity's size.

I Applicability

Applicability depends heavily on where the enterprise's traffic actually flows. A small firm with no servers on premises, a single internet connection and everything in SaaS will meet most of Control 13 through its SaaS security alerts, an EDR console and a managed firewall, and may reasonably mark 13.3, 13.8 and 13.9 as Not applicable only if it genuinely has no internal network worth protecting; a shared office LAN with printers and a NAS usually still counts. Cloud-heavy enterprises should look for the provider-native equivalents named in the Safeguards (cloud threat detection, flow logs, security groups, WAF) and confirm that every account and region is covered, not just production. Operational technology environments, such as a factory floor or a hospital's medical devices, need passive monitoring designed for industrial protocols and great care with inline prevention, because a blocked packet can stop a production line or a device; segmentation be-

tween IT and OT (13.4) is usually the highest-value step. Where monitoring is outsourced to an MSP, MSSP or MDR provider, the enterprise remains accountable: it should hold the contract terms on coverage, response times, data location and log retention, receive regular reports, and keep the right to see raw alerts and logs.

J Implementation Guidance

1. Confirm prerequisites: a current asset inventory (Control 1), a network diagram (12.4), a logging standard with sources and retention (Control 8) and synchronised time across devices. Monitoring an undocumented estate wastes effort.
2. Decide the operating model: in-house SOC, managed SOC or MDR, or a hybrid. Write down who watches alerts in and out of hours, the response target per severity and how alerts become incidents under Control 17.
3. Stand up central alerting (13.1) with the highest-value sources first, such as identity, VPN, firewall, EDR and cloud audit logs, and a modest starter rule set mapped to likely attacks.
4. Extend sensor coverage: host detection across servers and endpoints (13.2), network detection at chokepoints and cloud threat detection (13.3), and flow log export (13.6). Reconcile coverage against the asset inventory monthly.
5. Segment the network (13.4) using a zone model derived from data classification, and filter traffic between zones on a default-deny basis, giving priority to separating user devices from servers and IT from OT.
6. Apply posture checks to remote access (13.5) so that unhealthy or unmanaged devices receive limited access or none.
7. For IG3, move proven detections into prevention: EDR blocking (13.7), inline network prevention (13.8) and application layer filtering through proxy, WAF or API gateway (13.10), each piloted before enforcement.
8. For IG3, introduce port-level authentication (13.9) on wireless first and then on wired ports, with a controlled register of MAC-bypass devices.
9. Establish a monthly tuning cycle (13.11) with metrics on alert volume, false positives and missed detections, and feed lessons from incidents and penetration tests (Control 18) back into rules.
0. Report monitoring coverage and alert quality to management at least quarterly, including known blind spots and the plan to close them.

K Tools and Automation

- SIEM or log analytics platform: collects and correlates events from many sources, raises alerts and keeps searchable history for investigations and CERT-In retention. Open-source stacks such as Wazuh or an ELK-based build are workable for smaller budgets.
- EDR or host IPS agent: provides host-level detection (13.2) and, in blocking mode, prevention and isolation (13.7).
- Network IDS/IPS and network detection and response sensors: inspect traffic at chokepoints; Suricata and Zeek are widely used open-source engines.
- Flow collectors and cloud flow logs: give a cheap, high-coverage record of communications for hunting and exfiltration detection.
- Next-generation firewalls, internal segmentation firewalls and cloud security groups: enforce zone boundaries and, where licensed, application-aware rules.
- Network access control with RADIUS and PKI: authenticates devices at switch ports and wireless access points (13.9) and can quarantine non-compliant devices.
- Secure web gateway or filtering proxy, WAF, API gateway and DNS filtering: apply application layer controls (13.10).

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
CISO or security lead	Owns the monitoring strategy, approves the operating model and accepts residual blind spots
SOC analysts or MDR provider	Triage alerts within agreed targets, escalate incidents and record actions
Detection engineer	Writes and tunes correlation rules and thresholds, runs the monthly tuning review and maintains rule documentation
Network team	Implements segmentation, flow export, sensor placement, NAC and inline devices under change control
Endpoint team	Maintains host agent coverage and policy modes across servers and end-user devices

Role	Responsibility
Asset and application owners	Confirm business need for inter-zone flows and agree fail-open or fail-closed decisions

M Documentation and Records

- Network monitoring standard covering scope, log sources, sensor placement and retention
- SOC or MDR operating procedures, including severity definitions, response targets and escalation to incident response
- Network zone model and inter-zone flow matrix
- Remote access posture policy
- Correlation rule catalogue and tuning log
- NAC design and MAC-bypass register (IG3)
- Managed service contract and service reports where monitoring is outsourced

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 19-2. Assessment testing procedures, Control 13

Test ID	Method	Testing procedure	Result
TP-C13-01	**EXAMINE**	13.1: Examine the log source register and the SIEM or log analytics console. Compare the sources actually reporting against the critical asset list from the inventory and the logging standard, and identify any critical asset type (domain controllers, firewalls, VPN, cloud audit trails, email gateway, EDR) not forwarding events. Confirm that time stamps are synchronised and that silent-source alerting is configured.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-02	**SAMPLE**	13.1: Select a sample of alerts generated across the assessment period (for example 25 alerts spread across severities and months) and trace each to a ticket or case showing who received it, when it was acknowledged, what triage was done and how it was closed. Compare acknowledgement and closure times against the documented response targets.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-03	**INSPECT**	13.2: Inspect the host detection coverage report and reconcile it against the asset inventory for servers and end-user devices. Calculate coverage per asset group, and confirm that each uncovered asset is recorded as an approved exception with a compensating control. Inspect one server and one laptop directly to confirm the agent is installed, running and reporting.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-04	**EXAMINE**	13.3: Examine the network diagram and confirm network detection sensors or cloud-native threat detection are present at each chokepoint identified in the monitoring standard and in every cloud account or subscription in scope. Examine the signature update history for the period and confirm alerts from these sensors reach the central platform.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-05	**RE-PERFORM**	13.3: With written authorisation, generate benign test traffic that the sensors should detect (for example a published IDS test string or a controlled internal port scan from an approved host) and confirm an alert is raised and routed to the correct queue within the expected time.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-06	**INSPECT**	13.4: Inspect the zone model and a rule export from internal firewalls, layer-3 ACLs or cloud security groups. Confirm a default-deny stance between zones, identify any broad any-to-any or any-to-server rules, and select a sample of rules to verify they have an owner, a business justification and a review date. Examine evidence of the most recent rule review.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-07	**OBSERVE**	13.5: Observe a test remote connection from a device that fails a posture check (for example outdated anti-malware signatures or a missing patch, prepared with the IT team) and confirm it is blocked or restricted as the policy states. Examine posture logs for the period for denied or quarantined sessions and the exception list for approvals.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C13-08	**EXAMINE**	13.6: Examine the configuration of core network devices and cloud accounts for flow log export, and the collector or SIEM retention settings. Confirm retention meets the enterprise policy and the CERT-In 180-day expectation. Retrieve flow records for a date at least five months earlier to confirm they are actually retained and searchable, and confirm at least one flow-based alert rule is active.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-09	**INSPECT**	13.7: Inspect the EDR or host IPS policy for each asset group and confirm prevention mode is enabled for the behaviours the enterprise has chosen to block. Sample blocked or isolation events from the period and confirm each was reviewed. Identify any agents running in audit-only mode without an approved reason.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-10	**EXAMINE**	13.8: Examine the inline IPS or cloud inline protection policy, the record of which signatures are set to block, the decision on fail-open or fail-closed per device, and the change records for moving rules into prevention. Examine block logs for a sample month and evidence that they are reviewed.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-11	**OBSERVE**	13.9: Observe an unmanaged test laptop being connected to a wired port in a general office area and to the corporate wireless network, and confirm it is denied or placed in a guest or quarantine VLAN. Examine the MAC-bypass register and sample entries to confirm each is a documented device in a restricted segment.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-12	**INSPECT**	13.10: Inspect the web proxy or secure web gateway policy, and the WAF or API gateway configuration for a sample of internet-facing applications. Confirm application layer filtering is in blocking mode where intended, that TLS inspection decisions and exemptions are approved, and that blocked request logs are retained and reviewed.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-13	**SAMPLE**	13.11: For each month in the assessment period, obtain evidence of the tuning review (minutes, tickets or change records). Confirm no month is missing, that alert-quality metrics were considered and that a sample of threshold or suppression changes carry a recorded reason and approval. Challenge any broad suppressions that could hide genuine attacks.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C13-14	**INTERVIEW**	13.1, 13.11: Interview the SOC lead or MDR service manager about out-of-hours coverage, the most recent missed or late detection and what was changed as a result. Corroborate the answer against tuning records and the incident register.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Use a period-based approach: the assessment period is normally the last twelve months, or the period since monitoring went live if shorter. For alert handling (13.1), sample around 25 alerts weighted towards high and critical severities and spread across months, weekends and nights so that out-of-hours handling is tested. For coverage Safeguards (13.2, 13.7), reconcile the full population of agents against the full inventory rather than sampling, since tooling makes this cheap; then physically inspect two or three devices. For rule bases (13.4, 13.10), sample 15 to 25 rules, deliberately including the broadest rules and rules added most recently. For the monthly tuning Safeguard (13.11), inspect every month in the period; a single missing month is a partial implementation. Where monitoring is outsourced, add a sample of the provider's monthly service reports and compare their stated coverage with the enterprise's own inventory.

P Interview Questions

Interviewee	Question
CISO or security lead	Which parts of the estate are not monitored today, how were those blind spots accepted, and when will they close?

Interviewee	Question
SOC analyst or MDR contact	Walk me through the last high-severity alert you handled, from notification to closure. How did you decide whether it was an incident?
Detection engineer	How do you decide to raise a threshold or suppress a rule, and who checks that the change does not hide real attacks?
Network engineer	How is a new flow between two zones requested, approved and later removed?
Endpoint administrator	How would you know if an EDR agent on a server stopped reporting or was switched to audit-only mode?

Q Technical and Process Verification

- Coverage of central alerting, host sensors and network sensors is reconciled against the asset inventory, with exceptions approved.
- Alerts reach a named queue and are triaged within documented targets, including out of hours.
- Inter-zone filtering follows a default-deny approach with justified, reviewed rules.
- Remote devices that fail posture checks are blocked or restricted in practice, not only in policy.
- Flow and security logs are retained for the required period and can be searched.
- For IG3, prevention modes, port authentication and application layer filtering are enforced, and tuning occurs every month.

R Expected Evidence

- Log source register and SIEM health dashboard
- Agent and sensor coverage reconciliations against the asset inventory
- Network diagram showing zones, sensors and filtering points
- Firewall, security group and NAC configuration exports
- Remote access posture policy and denial logs
- Flow log configuration and retention evidence
- Sampled alert tickets with timestamps
- Monthly tuning records and rule change log
- Managed SOC or MDR contract and monthly service reports

S Evaluation Criteria

Implemented

- All critical log sources feed a central platform, correlation rules route alerts to owners, and sampled alerts were handled within target.
- Host and network sensor coverage is at or near the full in-scope population, with every gap documented and approved.
- Segmentation, remote posture and flow logging operate as designed and are evidenced over the period; for IG3, prevention, NAC, application layer filtering and monthly tuning are all evidenced.

Partially implemented

- A SIEM exists but important sources (for example cloud audit logs or VPN) are missing, or alerts are not consistently triaged.
- Segmentation exists on paper but broad rules allow most internal traffic between zones.
- Tuning happens irregularly, with some months missing or changes undocumented.

Not implemented

- Events are not collected centrally, or alerts go to an unmonitored mailbox.
- No host or network intrusion detection is deployed and the internal network is flat.
- Remote devices connect with no health checks.

T Common Gaps and Findings

- Condition: the SIEM receives logs from on-premises servers but not from the cloud tenant or SaaS identity provider. Criteria: 13.1 expects central alerting across enterprise assets. Effect: account takeover and cloud misuse would not raise an alert.
- Condition: EDR is installed on 70 per cent of laptops and 40 per cent of servers. Criteria: 13.2 and 13.7 expect host coverage wherever supported. Effect: attackers can operate on uncovered servers without detection.

- Condition: the internal network is a single VLAN with user laptops, servers and CCTV recorders. Criteria: 13.4 expects filtering between network segments. Effect: one compromised laptop can reach every server and device, enabling rapid ransomware spread.
- Condition: flow logs are kept for 30 days on the collector. Criteria: enterprise policy and the CERT-In 180-day expectation. Effect: investigations into slow-moving intrusions cannot reconstruct activity, and regulatory requests cannot be answered.
- Condition: no tuning review has been held for five months and 60 per cent of alerts are closed as false positives. Criteria: 13.11 expects monthly tuning. Effect: analysts suffer alert fatigue and genuine alerts are missed.
- Condition: VPN admits any device with valid user credentials. Criteria: 13.5 expects access based on device health. Effect: unpatched or infected personal devices gain full network access.

U Remediation Guidance

- Onboard the missing cloud and identity log sources to the SIEM within 30 days and add silent-source alerting.
- Set a coverage target for host agents (for example 98 per cent of supported assets) and track it weekly until achieved, recording exceptions formally.
- Introduce a basic zone model, separating at least users, servers, management and IoT or OT, and apply default-deny filtering between them in phases.
- Extend log and flow retention to meet policy and CERT-In expectations, using cheaper archive storage for older data.
- Institute a monthly tuning meeting with a fixed agenda and metrics, and require a documented reason for every suppression.
- Enable posture checks on the VPN or move to zero-trust access with device compliance conditions, starting with administrator and finance users.

V Monitoring Metrics

- Percentage of critical log sources reporting to the central platform in the last 24 hours (target 100 per cent).
- Host agent coverage as a percentage of supported servers and end-user devices in the inventory.
- Median time to acknowledge high and critical alerts, measured monthly against target.
- False-positive rate per correlation rule, and number of rules tuned each month.
- Number of broad inter-zone rules (any-to-any or any-to-server) remaining, trending to zero.

W Related Controls and Maturity Indicators

- Control 1 and Control 2 (asset and software inventories define what must be monitored)
- Control 4 (4.4 and 4.5 host and server firewalls; secure configuration baselines used in 13.5 posture checks)
- Control 8 (audit log collection, retention and review feed 13.1 and 13.6)
- Control 10 (malware defences overlap with 13.2 and 13.7)
- Control 12 (network infrastructure, architecture and segmentation underpin 13.4 and 13.9)
- Control 17 (alerts become incidents; 17.9 thresholds)
- Control 18 (18.4 uses penetration test results to improve detection rules)

Initial	Defined	Managed	Optimised
Firewall and endpoint protection exist, but alerts go to individual consoles or mailboxes and are reviewed only when something goes wrong. The internal network is largely flat.	A monitoring standard names log sources, sensors and response targets. A SIEM or managed service collects key sources, and a zone model and remote posture policy are documented, although coverage gaps remain.	Coverage is reconciled against the inventory, alerts are triaged within measured targets, segmentation and posture checks are enforced, and flow logs are retained and used. Prevention modes are enabled where justified.	Detection content is mapped to likely attack techniques, tuned monthly using metrics and test results, and validated through purple-team or penetration test feedback. Blind spots are few, known and shrinking.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A fictional 600-employee Pune NBFC runs its loan management system in a domestic cloud region, keeps a small on-premises server room for its branch network, and has 1,100 laptops across 70 branches. Its IT team had firewalls and an endpoint protection product, but each console sent alerts to a different mailbox. After a branch laptop was used to try credential stuffing against the loan portal one weekend, nobody noticed until Monday, and the CISO realised the CERT-In six-hour window would have been impossible to meet.

The NBFC chose a hybrid model: a managed MDR provider watching alerts around the clock, with an internal detection engineer owning rules and tuning. In the first quarter it onboarded identity, VPN, firewall, cloud audit and EDR logs to a SIEM hosted in India, enabled cloud flow logs and the provider's native threat detection, and set flow retention to 180 days with archive storage beyond that. EDR coverage was reconciled weekly against the asset inventory, rising from 72 to 97 per cent of laptops, with the remainder listed as exceptions.

In the second quarter the network team separated branch user VLANs from the server room and the CCTV network, replacing a single permissive rule with 41 named flows. VPN access now checks EDR status and patch level; failing laptops reach only a remediation portal. A monthly tuning review cut the false-positive rate on the top ten rules from 58 to 19 per cent.

The assessor sampled 25 alerts across the year and found two weekend alerts acknowledged outside target, leading to a finding against the MDR contract. 13.9 and 13.10 were rated partially implemented, since 802.1X covered wireless but not branch wired ports.

WP-C13: use the workpaper format shown in Appendix H.

CHAPTER 20 · CIS CONTROL 14

Security Awareness and Skills Training

CIS CONTROL 14 · 9 SAFEGUARDS · 8 IN IG1

Security Awareness and Skills Training

CIS Controls v8.1 · titles quoted verbatim | WP-C14

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 14 — Security Awareness and Skills Training

Control 14 deals with people. Technology can block much of what attackers try, but a great deal of real-world compromise still begins with a human decision: clicking a link, approving a login prompt, sending a file to the wrong address, plugging into café Wi-Fi or ignoring a warning that updates have failed. This Control asks the enterprise to run a deliberate programme that turns its workforce from an easy target into an early-warning network.

The Control is unusual in that eight of its nine Safeguards are in IG1. That reflects a simple judgement: even the smallest organisation cannot outsource human behaviour, and a few hours of well-designed training each year is among the cheapest defences available. The ninth Safeguard, role-specific training, adds depth for people whose access or authority makes them more valuable to an attacker.

A good programme is not a once-a-year slide deck. It is short, frequent, local and practical. It uses examples from the staff's own world, is delivered in languages they read comfortably, measures behaviour rather than attendance alone, and rewards reporting.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 20-1. Safeguards of CIS Control 14, Security Awareness and Skills Training

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
14.1	**“Establish and Maintain a Security Awareness Program”**	Documentation	Govern	IG1	Run a standing, owned programme that teaches every workforce member how to work safely with the organisation's systems and data. New joiners are trained before or soon after they get access, everyone is refreshed at least once a year, and the material itself is reviewed yearly or sooner when the business, its technology or its threats change materially.
14.2	**“Train Workforce Members to Recognize Social Engineering Attacks”**	Users	Protect	IG1	Teach staff to spot and resist manipulation: phishing and smishing, voice calls impersonating banks or senior people, business email compromise, fake vendor bank-change requests, pretext calls to the help desk and people following others through secured doors.
14.3	**“Train Workforce Members on Authentication Best Practices”**	Users	Protect	IG1	Make sure people understand how to protect their logins: why multi-factor authentication matters and how push-fatigue attacks work, how to build long passphrases, why passwords must not be reused or shared, and how to use the approved password manager.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
14.4	**“Train Workforce on Data Handling Best Practices”**	Users	Protect	IG1	Train people to recognise which information is sensitive under the organisation's classification scheme, and how to store, send, archive and destroy it correctly, including clean-desk and locked-screen habits and wiping whiteboards and shared screens after meetings.
14.5	**“Train Workforce Members on Causes of Unintentional Data Exposure”**	Users	Protect	IG1	Raise awareness of the ordinary mistakes that leak data without any attacker involved: auto-complete sending mail to the wrong person, losing a laptop or phone, sharing a cloud link as public, or posting screenshots and documents to the wrong audience.
14.6	**“Train Workforce Members on Recognizing and Reporting Security Incidents”**	Users	Protect	IG1	Equip every person to recognise the signs that something may be a security incident and to report it quickly through a known, easy route, without fear of blame.
14.7	**“Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates”**	Users	Protect	IG1	Teach users how to check that their device is receiving updates, what a failed or stuck update or a disabled security agent looks like, and that they must tell IT when they see it.
14.8	**“Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks”**	Users	Protect	IG1	Make people aware of the risks of using open or untrusted Wi-Fi and networks for work, and give remote and hybrid staff practical guidance on securing their home router and network.
14.9	**“Conduct Role-Specific Security Awareness and Skills Training”**	Users	Protect	IG2	Go beyond general awareness for people whose jobs carry higher risk or need specialist skill: administrators, developers, finance staff who approve payments, executives and their assistants, HR, helpdesk agents and OT engineers each receive training relevant to their duties.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
14.1	**1.** Write a one-page programme charter naming the owner (usually the CISO or IT head), the audiences, the minimum topics (14.2–14.8), the induction and annual refresher cadence, and how completion is tracked. **2.** Link induction training to the joiner workflow so that HR or IT cannot close onboarding until the module is complete or a dated exception is recorded. **3.** Build an annual calendar that mixes a formal refresher with short monthly nudges (posters, two-minute videos, WhatsApp or intranet tips) in English and the regional languages the workforce actually reads. **4.** Hold a yearly content review, and trigger an extra one after a significant incident, a merger, a new regulation or a major platform change; record what changed and why.	• Approved programme charter or policy section with owner, scope and cadence, showing the last review date. • Training-platform or attendance records showing induction and annual completion by person. • Content review log listing revisions made in the last twelve months.

Safeguard	Practical steps	Evidence
14.2	**1.** Build modules around real local lures: fake courier and GST notices, KYC-update SMS, 'CEO on WhatsApp needs gift cards', fake job offers and spoofed supplier invoices. **2.** Teach one simple rule set: pause, verify through a known channel, and report; reinforce that staff will not be blamed for reporting. **3.** Run periodic simulated phishing exercises with a report button, and coach repeat clickers privately rather than shaming them. **4.** Cover physical pretexting and tailgating at reception, plant gates and server rooms.	• Social-engineering module content and completion records. • Simulation campaign reports showing click, credential-entry and report rates over time. • Records of follow-up coaching for repeat clickers.
14.3	**1.** Explain MFA prompts in plain language, including never approving a prompt you did not trigger and never reading an OTP to a caller. **2.** Teach passphrase construction and the ban on reuse between work and personal accounts, aligned with the password standard under Control 5. **3.** Demonstrate the approved password manager and show how to store shared credentials in it rather than in spreadsheets or chat groups. **4.** Tell staff exactly how to report a suspected credential compromise and what will happen next.	• Authentication module content consistent with the current password and MFA standard. • Completion records. • Help-desk tickets showing staff-reported suspicious MFA prompts or credential exposure.
14.4	**1.** Map the data classification labels from Control 3 to everyday examples staff recognise: Aadhaar copies, salary sheets, customer KYC, drawings, patient records. **2.** Show the approved channel for each kind of transfer (managed file share, encrypted mail, secure portal) and what is banned (personal Gmail, unmanaged USB, consumer messaging). **3.** Teach retention and disposal: shredding bins, approved destruction of media, and not keeping personal copies. **4.** Reinforce clean-desk and screen-lock behaviour with periodic walk-round checks.	• Data-handling module mapped to the classification scheme. • Completion records. • Clean-desk walk-round results or screen-lock spot-check logs.
14.5	**1.** Use short case stories of mis-sent mail, open cloud links and lost devices, ideally anonymised from the organisation's own history. **2.** Teach checks before sending (recipients, attachments, link permissions) and the immediate steps if a mistake happens. **3.** Explain that under the DPDP regime a mis-sent personal-data file may itself be a reportable breach, so speed of reporting matters.	• Module content covering accidental disclosure scenarios. • Completion records. • Incident tickets showing self-reported accidental disclosures and how quickly they were raised.

Safeguard	Practical steps	Evidence
14.6	**1.** Publish one reporting route (phish button, short email alias, phone number, help-desk category) and repeat it in every module and on posters. **2.** List typical warning signs: unexpected MFA prompts, ransom notes, files renamed, mailbox rules nobody set, lost devices, unknown people in secure areas. **3.** Explain why time matters, including the CERT-In six-hour reporting expectation the organisation must meet. **4.** Test the route: send a dummy report and measure how long it takes to reach the incident handler.	• Incident-reporting module and poster or intranet page showing the route. • Completion records. • Reported-incident log with time from staff report to triage.
14.7	**1.** Show users where to see update status and last-update date on their operating system and on their phone. **2.** Describe warning signs: repeated failed-update notices, antivirus or EDR icons showing a warning, prompts to install 'urgent' updates from websites. **3.** Give a simple reporting route and confirm that IT acknowledges and acts on these reports.	• Module content with screenshots for the platforms in use. • Completion records. • Help-desk tickets raised by users about update or agent failures.
14.8	**1.** Explain the risks of hotel, airport, café and railway-station Wi-Fi, and the rule to use the corporate VPN or a mobile hotspot. **2.** Provide a home-network checklist: change the default router password, update firmware, use WPA2 or WPA3, separate guest devices where possible. **3.** Remind staff not to move enterprise data through personal cloud or file-sharing tools when working remotely.	• Remote-working and insecure-network module content including a home-router checklist. • Completion records for remote and hybrid workers. • Remote-working policy acknowledgements.
14.9	**1.** Identify high-risk roles from the access and payment-approval matrices and agree the learning objective for each. **2.** Provide targeted content: secure administration and privileged-access hygiene for IT, secure coding for developers (see 16.9), BEC and payment-verification drills for finance, deep-fake and whaling awareness for executives, caller verification for the help desk. **3.** Track role-based completion separately and refresh at least annually or on role change.	• Role-to-training matrix. • Completion records by role. • Certificates or attendance records for specialist courses.

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
IG1 enterprises must implement Safeguards 14.1 to 14.8. In practice this means a written, owned programme with induction and at least annual training (14.1) that covers social engineering (14.2), authentication habits (14.3), data handling and clean desk (14.4), accidental exposure (14.5), recognising and reporting incidents (14.6), reporting missing updates or failed security tools (14.7) and the risks of insecure networks, including home networks for remote staff (14.8). A 40-person firm can meet this with a two-hour annual session, a short induction module, a monthly tip and one phishing simulation per quarter.	IG2 adds 14.9: role-specific training for people whose duties carry higher risk, such as administrators, developers, finance approvers, executives and help-desk staff. IG2 enterprises are also expected to apply the IG1 Safeguards more systematically: tracked completion, measured behaviour (simulation click and report rates) and content refreshed from real incidents.	No IG3-only Safeguards. IG3 enterprises apply all nine Safeguards with greater rigour: risk-based targeting of training from incident and simulation data, advanced exercises for executives (deep-fake voice and video, whaling), tabletop drills that include non-IT staff, and behaviour metrics reported to the board.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 14.1 → 6.3 Information security awareness, education and training; clause 7.2 Competence; clause 7.3 Awareness; clause 7.4 Communication
- 14.2 → 6.3; 5.7 Threat intelligence (feeding current lures into content); 7.2 Physical entry (tailgating)
- 14.3 → 6.3; 5.17 Authentication information
- 14.4 → 6.3; 5.10 Acceptable use of information and other associated assets; 5.12 Classification of information; 5.14 Information transfer; 7.7 Clear desk and clear screen; 7.10 Storage media
- 14.5 → 6.3; 5.14 Information transfer; 8.1 User endpoint devices
- 14.6 → 6.8 Information security event reporting; 6.3
- 14.7 → 6.3; 8.1 User endpoint devices; 8.8 Management of technical vulnerabilities
- 14.8 → 6.7 Remote working; 6.3; 8.20 Networks security
- 14.9 → 6.3; clause 7.2 Competence; 8.28 Secure coding (developer training)

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: PR.AT-01 (personnel given awareness and training) for 14.1–14.8; PR.AT-02 (individuals in specialised roles trained) for 14.9; DE.AE and RS.MA touchpoints for 14.6 reporting (Srida IT mapping)
- NIST SP 800-53 Rev. 5: AT-2 Literacy training and awareness (including AT-2(3) social engineering), AT-3 Role-based training, AT-4 Training records, IR-6 Incident reporting
- NIST SP 800-50 Rev. 1 on building a cybersecurity and privacy learning programme, as background reading

F India Regulatory Touchpoints

- CERT-In Directions of 28 April 2022: reportable incidents must reach CERT-In within six hours of being noticed; this is achievable only if staff recognise and report events immediately (14.6).
- RBI cyber security and IT governance directions for banks and NBFCs expect awareness programmes for staff, senior management and the board, and in some cases customer awareness on frauds.
- SEBI Cybersecurity and Cyber Resilience Framework (CSCRF, 2024) includes training and awareness expectations for regulated entities' staff and specialised roles.
- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6 require reasonable security safeguards; trained staff and controls against accidental disclosure are evidence of them, and r.7 breach intimation depends on staff reporting mis-sends promptly.

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Social engineering, credential theft and simple human error appear again and again at the start of serious incidents. Business email compromise needs no malware at all: a convincing message asking accounts payable to change a supplier's bank details can move lakhs of rupees in minutes. Push-fatigue attacks rely on a tired user approving an MFA prompt. Ransomware often follows a single malicious attachment. In each case the user is the last control, and an untrained user is a control that fails silently.

Accidental exposure is just as damaging. A spreadsheet of customer KYC data sent to the wrong distribution list, a laptop left in a cab or a cloud folder shared as 'anyone with the link' can each create a personal-data breach. Under India's Digital Personal Data Protection regime such an event may need to be notified to the Data Protection Board and to affected individuals, and fines are tied to the failure to take reasonable security safeguards. Awareness training is part of what a regulator or auditor will expect to see as a reasonable safeguard.

In India the threat landscape has a strong local flavour: fake KYC and electricity-disconnection SMS, 'digital arrest' and courier-scam calls, fraudulent GST and income-tax notices, spoofed vendor invoices and WhatsApp impersonation of senior leaders. Training that uses imported, generic examples misses these. Regulators also expect training: RBI and SEBI frameworks for regulated entities call for awareness programmes, and CERT-In's six-hour reporting expectation only works if staff report quickly.

I Applicability

Control 14 applies to every enterprise regardless of size. A 40-person CA firm can run IG1 with free or low-cost material, a short annual session in the office and monthly email or WhatsApp tips; the key is to record who attended and to refresh the content each year. Cloud and SaaS-heavy firms should emphasise MFA fatigue, OAuth consent phishing and link-sharing settings. Manufacturers with OT and shop-floor staff need short, visual, regional-language content and should cover USB use on HMIs and contractor access to plant areas. Where IT is outsourced to an MSP, the enterprise still owns the programme; the MSP may deliver content or run simulations, but the enterprise must define scope, receive completion data and include MSP staff who hold privileged access in role-specific training (14.9).

J Implementation Guidance

1. Appoint a programme owner and agree a short charter covering audiences, minimum topics, cadence, languages and how success is measured.
2. Build or buy a baseline module set covering 14.2 to 14.8, localise it with Indian examples, and translate it for staff who do not read English comfortably.
3. Integrate induction training into onboarding so that access is not left running for untrained joiners beyond a defined grace period.
4. Publish a single, blame-free reporting route and repeat it everywhere: email footer, intranet, posters, induction and every module.
5. Run a phishing and smishing simulation programme with a reporting button; measure click, credential-entry and report rates, and coach rather than punish.
6. Identify high-risk roles and deliver role-specific training (14.9), including payment-verification drills for finance and caller-verification for the help desk.
7. Track completion per person and per role; chase overdue staff through line managers and report coverage to management monthly.
8. Review content at least annually and after significant incidents, new regulations or platform changes; feed real incidents and near-misses into new material.
9. Report programme metrics (coverage, simulation trends, time to report) to senior management and the board at least annually.

K Tools and Automation

- Learning management system (LMS) or a simple training register: assigns modules, records completion and produces evidence for audit.
- Phishing simulation platform, including open-source options such as GoPhish: runs controlled campaigns and measures click and report rates.
- Mail-client report button integrated with the security mailbox or ticketing tool: makes reporting a one-click habit and feeds triage.
- Intranet, digital signage and messaging channels: deliver short nudges between formal sessions.
- HR information system integration: drives joiner, mover and leaver triggers for training assignment.
- Survey and quiz tools: test understanding and capture feedback in local languages.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
Board / senior management	Approves the programme, completes executive-level training and receives annual effectiveness reporting.
CISO or IT head (programme owner)	Owns the charter, content, calendar, metrics and annual review.
HR	Triggers induction training, maintains workforce data, supports follow-up of overdue completions and includes training in performance processes where appropriate.
Line managers	Ensure their team completes training on time and model good reporting behaviour.

Role	Responsibility
Security operations or IT help desk	Receives and triages reports, gives feedback to reporters and supplies real lures for content.
Data Protection Officer or privacy lead	Contributes data-handling and accidental-disclosure content and confirms DPDP-related messaging.
All workforce members, contractors and interns	Complete required training and report suspected incidents promptly.

M Documentation and Records

- Security awareness programme charter or policy section (owner, scope, cadence, topics).
- Annual training calendar and content inventory with version and review dates.
- Role-to-training matrix for 14.9.
- Phishing simulation plan and rules of engagement approved by HR and legal.
- Training completion records and exception register.
- Incident-reporting guidance and posters.
- Annual programme effectiveness report to management.

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 20-2. Assessment testing procedures, Control 14

Test ID	Method	Testing procedure	Result
TP-C14-01	**EXAMINE**	14.1: Examine the awareness programme charter or policy. Confirm it names an owner, covers all workforce categories (employees, contractors, interns), specifies training at onboarding and at least yearly, and shows a content review within the last twelve months or after the latest significant change.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C14-02	**SAMPLE**	14.1: From HR records, sample 25 joiners across the last twelve months and confirm each completed induction training within the defined grace period. Sample 25 existing staff and confirm completion of the refresher within the last year. Record exceptions and whether they were approved.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C14-03	**EXAMINE**	14.2: Examine the social-engineering module and confirm it covers phishing, BEC, pretexting and tailgating with current, locally relevant examples. Examine reports for the simulation campaigns run in the period and confirm trends are tracked and repeat clickers are followed up.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C14-04	**EXAMINE**	14.3: Compare the authentication module with the current password and MFA standard (Control 5 and 6). Confirm it covers MFA prompt hygiene, passphrases, non-reuse and the approved password manager, and that no outdated guidance (such as forced frequent rotation contrary to the standard) remains.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C14-05	**OBSERVE**	14.4: Walk a sample of work areas outside office hours or at lunch and observe clean-desk and screen-lock behaviour, whiteboards in meeting rooms and the use of shredding bins. Examine the data-handling module and confirm it reflects the organisation's classification labels.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C14-06	**EXAMINE**	14.5: Examine the content for coverage of mis-delivered mail, lost devices and over-shared links. Examine incident records for accidental disclosures in the period and confirm they were self-reported and that lessons were fed back into content.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C14-07	**RE-PERFORM**	14.6: Interview a sample of ten staff from different functions and ask them how they would report a suspected incident. Submit a test report through the published route and measure time to acknowledgement by the incident handler. Confirm the module covers warning signs and reporting.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C14-08	**INTERVIEW**	14.7: Ask a sample of users to show where they would check update status on their device and what they would do if updates or the security agent failed. Examine help-desk tickets for user-raised update or agent failures and confirm they were actioned.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C14-09	**EXAMINE**	14.8: Examine the insecure-network and remote-working content and confirm it includes public Wi-Fi risks, VPN use and home-router guidance. Sample remote and hybrid workers and confirm completion.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C14-10	**SAMPLE**	14.9: Examine the role-to-training matrix. Sample administrators, developers, finance approvers, executives and help-desk agents and confirm each completed the role-specific training required for their role within the last year or since role change.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C14-11	**INSPECT**	14.1: Inspect the training platform or register for completeness: compare the list of active accounts in the directory with the list of people assigned training and identify active users who have never been assigned.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Sample from the population of active workforce members, including contractors and interns, over the last twelve months. For an organisation of up to 100 people, test every joiner and a minimum of 25 or 25 per cent of other staff, whichever is lower. For larger populations sample 25 to 40 people, stratified by function, location and employment type, with deliberate inclusion of high-risk roles for 14.9. For simulations, review every campaign in the period rather than a sample. For observation tests, cover at least two sites or floors where more than one exists. Record the population, sample selection method and exceptions in WP-C14.

P Interview Questions

Interviewee	Question
Programme owner	How do you decide what goes into next year's content, and what changed after the last review?
Finance approver	Walk me through what you do when a supplier emails asking to change their bank account.
Help-desk agent	How do you verify a caller who says they are a director and have lost their MFA device?
Shop-floor supervisor or branch staff	If you saw a stranger in a restricted area, or your PC showed a ransom message, who would you tell and how?
HR	What stops a new joiner from working for months without completing induction training?
Remote employee	What have you been told about securing your home Wi-Fi and router?

Q Technical and Process Verification

- Programme document exists, is approved and has been reviewed within twelve months.
- Completion data reconciles to the active workforce list with documented exceptions.
- Content covers each topic in 14.2 to 14.8 and is current.
- Staff interviewed can describe the reporting route without prompting.
- Simulation and reporting metrics are tracked and show action on results.
- Role-specific training exists and is completed for identified high-risk roles.

R Expected Evidence

- Approved awareness programme charter and annual calendar.
- LMS completion export reconciled to HR headcount.
- Module content or slide decks with version history.
- Phishing simulation reports for the period.
- Reported-incident log with timestamps.
- Clean-desk walk-round results.

- Role-to-training matrix and specialist training records.
- Annual effectiveness report to management.

S Evaluation Criteria

Implemented

- An approved programme covers all workforce categories with induction and at least annual training, and content was reviewed in the last year.
- Completion is at or above the target (for example 95 per cent) with exceptions tracked.
- Staff know and use the reporting route, and simulation data show measured improvement.
- Role-specific training is defined and delivered (IG2 and above).

Partially implemented

- Training exists but completion is not tracked, or contractors and interns are excluded.
- Content is generic or out of date, or misses one or more of the topics in 14.2 to 14.8.
- Simulations are run but results are not acted on.

Not implemented

- No defined programme; training is ad hoc or limited to a policy acknowledgement.
- No records of who has been trained.
- Staff cannot describe how to report an incident.

T Common Gaps and Findings

- Condition: induction training is optional and 30 per cent of joiners in the sample had not completed it after three months. Criteria: 14.1 expects training at hire. Effect: new staff, often the most targeted, work without basic awareness.
- Condition: contractors and outsourced help-desk staff are not enrolled in the LMS. Criteria: 14.1 covers the whole workforce. Effect: people with real access to systems and data are untrained.
- Condition: no simulation or behaviour metric exists; success is measured only by attendance. Criteria: an effective programme under 14.1 and 14.2 should show behaviour change. Effect: management cannot tell whether training works.
- Condition: finance staff have had no training on verifying bank-detail changes. Criteria: 14.2 and 14.9. Effect: high exposure to business email compromise fraud.
- Condition: the reporting route differs between posters, the intranet and the incident policy. Criteria: 14.6. Effect: delayed reporting that endangers the six-hour CERT-In timeline.

U Remediation Guidance

- Make induction training a mandatory step in the onboarding checklist with an automated reminder and a defined grace period.
- Extend LMS enrolment to contractors, interns and MSP staff through the vendor contract and the joiner process.
- Start a quarterly simulation programme with a report button and report click, credential-entry and report rates to management.
- Introduce a call-back verification procedure for all bank-detail changes and train finance staff on it with a live drill.
- Standardise one reporting route across all channels and test it twice a year.

V Monitoring Metrics

- Percentage of the active workforce (including contractors) with current annual training; target at least 95 per cent.
- Percentage of joiners completing induction within the grace period; target 100 per cent.
- Phishing simulation report rate versus click rate per quarter; target a rising report rate and click rate below an agreed threshold.
- Median time from a user reporting a suspected incident to triage by the incident handler.
- Percentage of high-risk roles with completed role-specific training in the last twelve months.

W Related Controls and Maturity Indicators

- 3.1 and 3.7 (data management and classification that training explains)
- 5.2 and 6.3–6.5 (password and MFA standards behind 14.3)
- 7.3–7.4 and 10.1 (patching and anti-malware that 14.7 asks users to watch)
- 12 and 13 (network controls behind 14.8)
- 16.9 (developer training, a specialised form of 14.9)

- 17.3 (incident reporting process that 14.6 feeds)

Initial	Defined	Managed	Optimised
Training is ad hoc, usually a policy acknowledgement at joining; no completion tracking or metrics.	A documented programme with induction and annual training covers 14.2–14.8; completion is recorded.	Completion is tracked against headcount with escalation; simulations and reporting metrics guide content; role-specific training is delivered.	Training is targeted using incident, simulation and threat-intelligence data; behaviour metrics are reported to the board; staff reporting is a measurable detection source.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A 300-employee Coimbatore textile exporter handled payments to some 150 overseas buyers and local job-workers through two accounts staff. In one quarter it received three emails, apparently from long-standing suppliers, asking to switch payment to new bank accounts. One payment of about ₹18 lakh went out before the fraud was noticed. The company had a policy acknowledgement at joining but no training programme.

The IT manager, acting as programme owner, built a modest programme. Induction training became a mandatory step in the HR joining checklist, delivered as a 40-minute Tamil and English session with locally relevant examples: fake export-incentive notices, courier scams, WhatsApp messages purporting to come from the managing director, and supplier bank-change emails. An annual refresher was scheduled each April, with a monthly two-minute tip shared through the staff WhatsApp group and printed for the weaving and processing units.

For 14.9, the accounts team, the purchase team and the managing director's office received a separate session and a written call-back rule: no change to a supplier's bank details without confirmation through a phone number already on file, signed off by a second person. A free phishing simulation tool was used quarterly; the first campaign saw 31 per cent of recipients click and 4 per cent report. After a year the click rate was 9 per cent and the report rate 38 per cent.

When the next bank-change email arrived, the accounts executive called the supplier on the known number, confirmed it was fraudulent and reported it within twenty minutes. The IT manager blocked the sending domain and shared the lure in the next monthly tip. The assessor rated 14.1 to 14.8 Implemented and 14.9 Partially implemented, because developers at the firm's small ERP support vendor had not been included.

WP-C14: use the workpaper format shown in Appendix H.

CHAPTER 21 · CIS CONTROL 15

Service Provider Management

CIS CONTROL 15 · 7 SAFEGUARDS · 1 IN IG1

Service Provider Management

CIS Controls v8.1 · titles quoted verbatim WP-C15

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 15 — Service Provider Management

Control 15 is about the organisations an enterprise relies on but does not run: cloud and SaaS platforms, managed service providers, payroll bureaus, call centres, software vendors with support access, logistics partners, auditors and freelance consultants. Each one can hold enterprise data or reach enterprise systems, and each one's security failure can become the enterprise's incident.

The Control follows a life cycle. It starts with knowing who the providers are (15.1), sets the rules in a policy (15.2), ranks providers by risk (15.3), writes security into contracts (15.4), checks providers before and during the relationship (15.5 and 15.6) and closes relationships cleanly (15.7). Only the inventory is in IG1; the governance Safeguards come in at IG2 and the assurance and offboarding work at IG3, because the effort scales with the number and criticality of providers.

Responsibility cannot be outsourced. Indian regulators are explicit that a regulated entity remains accountable for outsourced activities, and under the DPDP Act a Data Fiduciary remains responsible for processing done on its behalf by a Data Processor.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 21-1. Safeguards of CIS Control 15, Service Provider Management

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
15.1	**“Establish and Maintain an Inventory of Service Providers”**	Users	Identify	**IG1**	Keep a single, current list of every external party that provides services to the organisation or holds, processes or can reach its data or systems. Each entry records what the provider does, how it is classified and which named internal person is accountable for the relationship. The list is reviewed at least yearly and whenever the business changes significantly.
15.2	**“Establish and Maintain a Service Provider Management Policy”**	Documentation	Govern	**IG2**	Adopt an approved policy that governs the whole provider life cycle: how providers are classified and inventoried, what due diligence is needed before engagement, how they are monitored while in service and how the relationship is closed down securely. The policy is reviewed at least yearly or after significant change.
15.3	**“Classify Service Providers”**	Users	Govern	**IG2**	Rank providers into tiers by the risk they bring, considering the sensitivity and amount of data they touch, how much the business depends on their availability, the regulations that apply, their inherent risk and the controls that offset it. Tiers are revisited at least yearly or on significant change.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
15.4	**“Ensure Service Provider Contracts Include Security Requirements”**	Documentation	Govern	IG2	Make sure each contract with a provider carries security obligations proportionate to its tier and consistent with the policy: baseline security controls, incident and breach notification within set times, encryption, audit and inspection rights, sub-contracting limits, and return or destruction of data at exit. Contracts are reviewed at least yearly for missing clauses.
15.5	**“Assess Service Providers”**	Users	Govern	IG3	Carry out a risk-based security assessment of providers in line with the policy, before engagement and then at least yearly or at contract renewal. The depth varies by tier and may rely on independent assurance reports, tailored questionnaires, evidence review or on-site audits.
15.6	**“Monitor Service Providers”**	Data	Govern	IG3	Watch providers continuously between formal assessments: track service and security performance, follow their release notes and security advisories, monitor for breaches, leaked credentials or data involving them, and reassess when risk signals appear.
15.7	**“Securely Decommission Service Providers”**	Data	Protect	IG3	When a provider relationship ends or a service is withdrawn, close it securely: disable the provider's user, service and API accounts, cut connections and data feeds, recover assets, and obtain return or verified destruction of the organisation's data, including copies held by sub-processors.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
15.1	1. Pull candidates from accounts-payable vendor masters, purchase orders, corporate card statements, SSO and OAuth app lists, firewall and VPN allow-lists and contracts held by legal. 2. Record for each provider: legal name, service, data categories and volume, systems connected, contract dates, classification, internal owner and security contact. 3. Include free and click-through SaaS, MSPs, payroll processors, cloud hosting, couriers that handle documents, auditors and individual consultants with remote access. 4. Review the inventory annually and on events such as a new business line, an acquisition or a change of core platform.	• Current service provider inventory with owner and classification columns populated. • Reconciliation of the inventory against vendor-payment and SSO application lists. • Dated record of the last annual review.
15.2	1. Define the life-cycle stages (identify, classify, assess, contract, onboard, monitor, offboard) and who approves at each. 2. Set minimum requirements per classification tier, including assessment depth, contract clauses and review frequency. 3. Align the policy with regulator expectations that apply, such as RBI outsourcing directions for banks and NBFCs or SEBI CSCRF third-party provisions, and DPDP processor obligations. 4. Obtain management approval and set an annual review date.	• Approved service provider management policy with version and review history. • Procedure or RACI showing approvals at each life-cycle stage. • Board or committee minutes where required by regulation.

Safeguard	Practical steps	Evidence
15.3	**1.** Agree three or four tiers (for example Critical, High, Medium, Low) with clear criteria. **2.** Score each provider with a short questionnaire: personal or financial data, privileged access, single point of failure, regulatory relevance, location of data. **3.** Flag providers that are material outsourcing under RBI directions or that are DPDP Data Processors handling personal data. **4.** Re-score at the annual review, at contract renewal and when the service scope changes.	• Classification criteria document. • Completed classification scoring for a sample of providers. • Evidence of re-classification after scope changes.
15.4	**1.** Maintain a standard security schedule or data processing agreement with clauses graded by tier. **2.** For DPDP Data Processors, include processing only on documented instructions, reasonable security safeguards, breach notification to the fiduciary without delay, sub-processor controls and erasure at the end of the engagement. **3.** Require incident notification fast enough for the organisation to meet CERT-In six-hour reporting and any sector regulator timelines. **4.** Run an annual contract review that compares live contracts against the current clause library and records remediation actions.	• Clause library or standard security schedule. • Sample executed contracts containing tiered security clauses. • Annual contract-gap review record.
15.5	**1.** Define the assessment pack per tier: critical providers might need an independent report (SOC 2 Type II, ISO/IEC 27001 certificate with scope statement, PCI DSS AoC) plus a questionnaire and evidence review; low-tier providers a short self-attestation. **2.** Check the scope and period of any certificate or report against the actual service being bought, and read the exceptions. **3.** For regulated entities, include on-site or remote audits where outsourcing rules call for them. **4.** Record findings, agree remediation with the provider and track it to closure.	• Completed assessments with dates and assessor. • Copies of independent assurance reports reviewed, with scope checked. • Findings tracker with provider remediation status.
15.6	**1.** Set monitoring activities per tier: SLA and security KPI reports, quarterly service reviews, subscribed security advisories, news and breach alerts. **2.** Use threat-intelligence or dark-web monitoring services, where proportionate, to detect leaked credentials or data tied to the organisation's providers. **3.** Monitor technical signals: provider accounts and connections in the organisation's own logs, certificate expiry, external attack-surface changes. **4.** Trigger out-of-cycle reassessment on breaches, ownership changes, material sub-contracting or repeated SLA failure.	• Service review minutes and KPI reports for critical providers. • Alert records from advisory, breach or dark-web monitoring and the actions taken. • Out-of-cycle reassessment records.

Safeguard	Practical steps	Evidence
15.7	1. Use an offboarding checklist triggered by contract termination or non-renewal, owned by the relationship owner. 2. Revoke accounts, keys, certificates, VPN and firewall rules, OAuth grants and API tokens; rotate any shared secrets the provider knew. 3. Stop data flows and integrations, and update the data-flow diagrams and inventories. 4. Obtain a written certificate of return or destruction covering backups and sub-processors, and update the provider inventory.	• Completed offboarding checklists for terminated providers. • Access-removal evidence (directory, VPN, firewall, SaaS admin logs). • Data return or destruction certificates.

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
IG1 enterprises must implement 15.1: a maintained inventory of service providers with a classification and a named internal owner for each, reviewed at least annually. For a 40-person firm this can be a spreadsheet of 20 to 60 rows built from the vendor-payment list and the SaaS apps staff sign into, with a simple High, Medium, Low label.	IG2 adds governance: an approved service provider management policy (15.2), a defined classification method (15.3) and security requirements in contracts consistent with that policy and reviewed annually (15.4). IG2 enterprises should be able to show which providers are critical and that critical contracts carry incident-notification, encryption and data-disposal clauses.	IG3 adds assurance and exit: risk-based assessment of providers before engagement and at least annually (15.5), ongoing monitoring between assessments (15.6) and secure decommissioning when relationships end (15.7). Regulated Indian entities subject to RBI or SEBI third-party requirements will often need IG3-level practices regardless of their overall IG choice.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 15.1 → 5.19 Information security in supplier relationships; 5.9 Inventory of information and other associated assets; 5.23 Information security for use of cloud services
- 15.2 → 5.19; 5.1 Policies for information security; 5.23
- 15.3 → 5.19; 5.21 Managing information security in the ICT supply chain; clause 6.1.2 Information security risk assessment
- 15.4 → 5.20 Addressing information security within supplier agreements; 5.21; 5.31 Legal, statutory, regulatory and contractual requirements; 5.34 Privacy and protection of PII
- 15.5 → 5.19; 5.21; 5.22 Monitoring, review and change management of supplier services
- 15.6 → 5.22; 5.7 Threat intelligence
- 15.7 → 5.22; 5.11 Return of assets; 5.18 Access rights; 8.10 Information deletion

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: GV.SC-01 to GV.SC-10 (cybersecurity supply chain risk management); in particular GV.SC-04 (suppliers known and prioritised by criticality) for 15.1 and 15.3, GV.SC-05 (requirements in contracts) for 15.4, GV.SC-06 and GV.SC-07 (due diligence and ongoing risk management) for 15.5 and 15.6, GV.SC-10 (post-relationship provisions) for 15.7; ID.AM-04 (inventories of supplier services) for 15.1 (Srida IT mapping)
- NIST SP 800-53 Rev. 5: SR family (supply chain risk management), SA-9 External system services, SA-4 Acquisition process, PS-7 External personnel security
- NIST SP 800-161 Rev. 1 cybersecurity supply chain risk management practices, as background

F India Regulatory Touchpoints

- RBI Master Direction on Outsourcing of Information Technology Services (2023) for banks, NBFCs and other regulated entities: inventory of IT service providers, materiality assessment, due diligence, mandatory contract clauses including RBI audit and inspection access, monitoring, business continuity and exit strategy.
- DPDP Act 2023 s.8(2) (Data Processor engaged only under a valid contract), s.8(5) (reasonable security safeguards, including by processors) and s.8(7) (erasure, including by processors), read with DPDP Rules 2025 r.6 security safeguards, which expect appropriate contractual provisions with processors.
- SEBI CSCRF (2024): third-party and vendor risk management obligations for regulated entities, including expectations on outsourced IT and cloud services.
- CERT-In Directions of 28 April 2022: data centres, cloud, VPN and other service providers have their own reporting and log-retention duties; contracts should require incident cooperation within the six-hour window.

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Many significant incidents enter through a third party: a managed service provider whose remote-management tool is hijacked, a software vendor whose update channel is poisoned, a SaaS platform whose misconfigured storage leaks customer files, or a small contractor whose stolen VPN password opens the network. Attackers favour providers because one compromise can reach many customers. An enterprise that does not know which providers have access, what they hold and what they are obliged to do cannot react quickly when a provider is breached.

Weak provider management also turns into legal and financial exposure. Contracts without breach-notification clauses leave the enterprise unaware of incidents it is legally required to report. Data left behind with a former vendor remains the enterprise's liability. Providers that quietly sub-contract can move data to places the enterprise never approved.

In India these points carry regulatory weight. RBI directions on outsourcing of IT services require regulated entities to keep an inventory of IT service providers, to assess materiality, to carry out due diligence, to include specific clauses (including audit and inspection rights for the RBI), and to manage concentration and exit risk. SEBI CSCRF places third-party risk obligations on regulated entities. The DPDP Act 2023 requires a Data Fiduciary to engage a Data Processor only under a valid contract, and to ensure reasonable security safeguards and erasure of personal data, including by its processors. CERT-In Directions apply to service providers as well as their customers, so contracts must make reporting cooperation explicit.

I Applicability

Every organisation has service providers, so 15.1 applies to all. Small firms often depend on a handful of critical providers (email and office suite, accounting software, an IT support contractor, a payroll bureau) and can manage them through a short spreadsheet and a standard one-page security clause. Cloud and SaaS-heavy organisations should treat their hyperscaler and key SaaS platforms as critical providers and should rely on independent assurance reports scoped to the services used. Manufacturers with OT must include OEM and system-integrator remote access to plant systems, which is often the riskiest provider relationship they have. Where an MSP runs IT, the MSP itself is a critical provider, and its own subcontractors and remote-management tools fall within scope. Regulated financial entities must layer RBI, SEBI or IRDAI outsourcing requirements on top of this Control.

J Implementation Guidance

1. Build the provider inventory from finance, procurement, legal, SSO and network sources and assign an internal owner to each provider.
2. Draft and approve a service provider management policy covering the whole life cycle, mapped to applicable Indian regulatory requirements.
3. Define classification criteria and tier every provider, flagging DPDP Data Processors and RBI material outsourcing where relevant.
4. Create a clause library or security schedule graded by tier, including DPDP processor terms and incident-notification timelines that support CERT-In reporting.
5. Review existing critical and high-tier contracts against the clause library and plan amendments at renewal.
6. Design an assessment pack per tier and assess critical providers first, checking the scope and period of independent reports.

7. Set up monitoring: quarterly service reviews, advisory subscriptions, breach and credential-leak alerts, and triggers for out-of-cycle reassessment.
8. Introduce an offboarding checklist and run it for every terminated provider, obtaining data return or destruction certificates.
9. Report the provider risk position (critical providers, overdue assessments, open findings, concentration risk) to management at least annually.

K Tools and Automation

- Vendor or third-party risk management (TPRM) platform, or a structured spreadsheet for small firms: holds the inventory, tiers, assessment status and findings.
- Contract lifecycle management system or legal repository: stores contracts with tagged security clauses and renewal dates.
- SSO and SaaS management or CASB tooling: discovers SaaS providers in use and OAuth grants that represent provider access.
- Security questionnaire and evidence-exchange tools: standardise assessments and track responses.
- Threat intelligence, breach-alert and dark-web monitoring services: signal provider compromises and leaked credentials.
- PAM and remote-access gateways: control and record provider sessions and make offboarding verifiable.
- External attack-surface management tools: observe changes in internet-facing provider assets that serve the organisation.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
Board / risk committee	Approves the policy and, for regulated entities, material outsourcing arrangements; receives provider risk reports.
CISO or IT head	Owns the security requirements, assessment method and monitoring; signs off on critical provider assessments.
Procurement	Ensures no provider is engaged without inventory entry, classification and the required assessment.
Legal / company secretary	Maintains the clause library, negotiates security and DPDP processor terms, holds executed contracts.
Relationship (business) owner	Accountable for each provider day to day, runs service reviews and triggers offboarding.
Data Protection Officer or privacy lead	Confirms DPDP processor terms, sub-processor approvals and erasure at exit.
IT operations	Grants and revokes provider access, monitors provider connections and executes technical offboarding.

M Documentation and Records

- Service provider inventory.
- Service provider management policy and procedure.
- Classification criteria and scoring records.
- Security clause library and standard data processing agreement.
- Assessment questionnaires, completed assessments and findings tracker.
- Monitoring plan and service review minutes for critical providers.
- Offboarding checklist and completed records with destruction certificates.
- Regulator-required outsourcing registers or board approvals where applicable.

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 21-2. Assessment testing procedures, Control 15

Test ID	Method	Testing procedure	Result
TP-C15-01	EXAMINE	15.1: Examine the provider inventory and confirm each entry has a classification and a named internal owner, and that it was reviewed within the last twelve months.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C15-02	RE-PERFORM	15.1: Independently compile a list of providers from the last twelve months of vendor payments, the SSO application list and firewall or VPN rules for third parties. Compare with the inventory and record providers that are missing.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C15-03	EXAMINE	15.2: Examine the service provider management policy. Confirm it covers classification, inventory, assessment, monitoring and decommissioning, is approved, and was reviewed within the last twelve months or after the latest significant change. For regulated entities, compare it with the applicable RBI, SEBI or IRDAI requirements.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C15-04	SAMPLE	15.3: Sample 10 to 15 providers across tiers and re-perform the classification using the documented criteria. Confirm the assigned tier matches and that classifications were reviewed in the last year or after scope changes.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C15-05	SAMPLE	15.4: For a sample of critical and high-tier contracts, inspect the executed agreement and confirm it includes the clauses the policy requires for that tier: security baseline, breach notification timeline, encryption, audit rights, sub-contracting control and data return or destruction. For DPDP Data Processors confirm processor-specific terms.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C15-06	EXAMINE	15.4: Examine the record of the annual contract review and confirm gaps identified were assigned and tracked.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C15-07	SAMPLE	15.5: Sample critical providers and confirm an assessment was completed before engagement and within the last twelve months or at the latest renewal. Where independent reports were relied on, confirm that their scope covers the service bought, the period is current, and exceptions and complementary user-entity controls were evaluated.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C15-08	INTERVIEW	15.6: Interview relationship owners of critical providers about how they monitor service and security performance. Examine service review minutes, advisory or breach-alert records, and confirm at least one alert in the period led to a documented action or reassessment.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C15-09	SAMPLE	15.7: Sample providers terminated in the period. Inspect directory, VPN, firewall and SaaS admin evidence to confirm accounts and connections were removed by the agreed date, and confirm a data return or destruction certificate was obtained.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C15-10	INSPECT	15.7: Inspect active directory and remote-access accounts for third parties and confirm each maps to a current provider in the inventory; report orphaned provider accounts.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Sampling Guidance

Test the inventory in full by reconciliation against independent sources. For contract, assessment and monitoring tests, sample all critical providers where there are fewer than ten, otherwise at least ten critical plus five high-tier providers. For offboarding, test every provider terminated in the last twelve months up to 15, and a sample of 15 beyond that. Include at least one cloud or SaaS provider, one MSP or IT support provider and, where relevant, one OT integrator and one DPDP Data Processor. Record populations and selections in WP-C15.

P Interview Questions

Interviewee	Question
Procurement	Can a department sign up for a new SaaS tool on a company card without IT or security knowing? How would you find out?
Legal	Which clauses do you treat as non-negotiable for a provider that handles customer personal data?
CISO	When you rely on a SOC 2 report or ISO certificate, how do you check that it covers the service you actually use?
Relationship owner	How would you learn that your provider had been breached, and how quickly?
IT operations	When the last support vendor left, what did you disable and how did you prove it?
DPO or privacy lead	How do you know which sub-processors your processors use and where the data sits?

Q Technical and Process Verification

- Inventory is complete when reconciled to payments, SSO and network sources.
- Policy is approved, current and covers the full life cycle.
- Classification is consistently applied and re-performed results match.
- Critical contracts contain required security and DPDP processor clauses.
- Critical providers are assessed and monitored within the policy's intervals.
- Terminated providers no longer have access, and data return or destruction is evidenced.

R Expected Evidence

- Provider inventory export with owner and tier.
- Reconciliation workpaper against payments and SSO lists.
- Approved policy and procedure.
- Classification scoring sheets.
- Executed contracts or extracts showing security clauses.
- Assessment files, independent assurance reports and findings tracker.
- Service review minutes and monitoring alerts.
- Offboarding checklists, access-removal logs and destruction certificates.

S Evaluation Criteria

Implemented

- Inventory is complete, classified, owned and reviewed annually (IG1).
- Policy, classification and contract clauses are in place and applied to all critical providers (IG2).
- Critical providers are assessed, monitored and offboarded according to policy with evidence (IG3).

Partially implemented

- Inventory exists but misses SaaS, free tools or individual contractors, or lacks owners.
- Policy exists but contracts signed before it lack security clauses with no remediation plan.
- Assessments rely on certificates without checking scope or period.

Not implemented

- No inventory of service providers.
- No security requirements in provider contracts.
- Former providers retain access or data with no evidence of removal.

T Common Gaps and Findings

- Condition: 14 SaaS tools paid by corporate card are absent from the inventory. Criteria: 15.1 expects all known providers to be listed. Effect: personal data is processed by unassessed providers without contracts.
- Condition: the payroll bureau contract has no breach-notification clause. Criteria: 15.4 and DPDP processor obligations. Effect: the organisation may miss its own breach-intimation and CERT-In reporting duties.
- Condition: the main cloud provider is assessed by reference to an ISO/IEC 27001 certificate whose scope excludes the region used. Criteria: 15.5. Effect: false assurance about controls over the hosted data.
- Condition: an ERP support vendor terminated eight months ago still has an active VPN account. Criteria: 15.7. Effect: an unmonitored path into the network that an attacker could use.

- Condition: no monitoring of provider breach announcements. Criteria: 15.6. Effect: the organisation learns of provider compromise late, from the press.

U Remediation Guidance

- Reconcile the inventory quarterly against card and vendor payments and SSO logs, and block new SaaS purchases that bypass registration.
- Issue contract addenda with the standard security schedule and DPDP processor terms to all critical and high-tier providers at the next renewal or sooner.
- Re-perform assessments for critical providers with scope-checked assurance reports and targeted questionnaires.
- Run an immediate review of third-party accounts and disable all accounts not mapped to a current provider; make off-boarding a contract-termination trigger.
- Subscribe to provider security advisories and a breach-alert feed, and define reassessment triggers.

V Monitoring Metrics

- Percentage of providers in the inventory with a current tier and named owner; target 100 per cent.
- Percentage of critical providers with a contract containing all required security clauses; target 100 per cent.
- Percentage of critical providers assessed within the last twelve months.
- Number of third-party accounts not mapped to an active provider (target zero).
- Median days from provider termination to confirmed access removal and data destruction certificate.

W Related Controls and Maturity Indicators

- 1.1 and 2.1 (assets and software that providers supply or manage)
- 3.1–3.3 and 3.5 (data inventory, access and disposal that contracts must reflect)
- 5.1, 5.3 and 6.1–6.2 (provider accounts and revocation)
- 12.7 and 13 (provider remote access and monitoring)
- 16.4–16.5 (third-party software components and suppliers of code)
- 17.4 and 17.6 (incident response that relies on provider cooperation)

Initial	Defined	Managed	Optimised
Providers are engaged by individual departments; no central list; contracts are the provider's standard terms.	An inventory and policy exist; providers are tiered; a security clause library is used for new contracts.	Critical providers are assessed before engagement and annually, monitored through service reviews and alerts, and offboarded with evidence; metrics are reported.	Provider risk is managed as a portfolio, including concentration and fourth-party risk; continuous monitoring feeds automatic reassessment; exit plans for critical providers are tested.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A 600-employee Pune NBFC used 85 service providers, including a core lending platform hosted by its vendor, a cloud provider, a collections call centre, a document-storage firm, a KYC-verification API and an MSP that ran its desktops. An RBI inspection observation and the coming DPDP obligations prompted a review.

The CISO and the company secretary first rebuilt the inventory from accounts-payable data, purchase orders and the SSO console, and found 23 providers no one had recorded, mostly SaaS tools used by marketing and collections. Each provider was given an owner and a tier using a six-question score covering personal data, financial data, privileged access, business criticality, regulatory relevance and data location. Eleven came out as critical; seven of these were flagged as material IT outsourcing under the RBI directions and nine as DPDP Data Processors.

The board approved a revised policy linking these tiers to assessment depth and contract clauses. Legal prepared a security schedule with breach notification within a few hours to support CERT-In and DPDP timelines, encryption, RBI audit access, sub-processor approval and certified data destruction at exit. Critical contracts were amended within six months.

Assessments followed. The call centre provided an ISO/IEC 27001 certificate, but its scope covered only the Mumbai site while the work ran from Nashik; the NBFC required a supplementary questionnaire and a remote evidence review, which found shared agent logins. The finding was fixed within 60 days.

During offboarding of a former document-scanning vendor, IT found two VPN accounts still active a year after exit; they were closed and the offboarding checklist was tied to the contract-termination workflow. The assessor rated 15.1 to 15.5 and 15.7 Implemented and 15.6 Partially implemented, since breach-alert monitoring covered only critical providers' names and not their key sub-processors.

WP-C15: use the workpaper format shown in Appendix H.

CHAPTER 22 · CIS CONTROL 16

Application Software Security

CIS CONTROL 16 · 14 SAFEGUARDS · 0 IN IG1

Application Software Security

CIS Controls v8.1 · titles quoted verbatim | WP-C16

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 16 — Application Software Security

Control 16 covers the security of software the enterprise builds, customises, commissions or hosts: customer portals and mobile apps, internal web tools, APIs, ERP customisations, scripts and integrations, and increasingly code produced with AI assistance. Applications are where attackers meet the business logic and the data directly, and flaws in them cannot be fixed by patching the operating system or firewall.

All fourteen Safeguards sit in IG2 or IG3, because the Control assumes the enterprise develops or maintains software. An IG1 enterprise that buys only off-the-shelf software has little to do here beyond Controls 2, 7 and 15; but as soon as it has a developer, a web agency building its site or an outsourced team customising its ERP, IG2 expectations start to apply.

The Safeguards fall into four groups. Governance sets the process: the secure SDLC (16.1), vulnerability intake (16.2), root-cause analysis (16.3) and severity rating (16.6). Supply chain manages third-party code: component inventory (16.4) and trusted components (16.5). Engineering builds security in: hardened platforms (16.7), separated environments (16.8), trained developers (16.9), secure design (16.10) and vetted security modules (16.11). Verification at IG3 tests the result: automated code checks (16.12), penetration testing (16.13) and threat modelling (16.14).

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 22-1. Safeguards of CIS Control 16, Application Software Security

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
16.1	**“Establish and Maintain a Secure Application Development Process”**	Documentation	Govern	IG2	Define and keep current a documented secure development life cycle (SDLC) that every team building or customising software follows. It sets design and coding standards, developer training, how vulnerabilities are handled, how third-party code is controlled and what security testing happens before release. It is reviewed at least yearly or after significant change.
16.2	**“Establish and Maintain a Process to Accept and Address Software Vulnerabilities”**	Documentation	Govern	IG2	Operate a process for receiving and resolving software vulnerability reports from inside and outside the organisation, including a published route for external researchers and customers. The process names who handles reports, how they are logged, triaged, assigned, fixed and verified, and uses a tracking system with severity ratings and timing measures. It is reviewed at least yearly; software vendors should treat it as a public commitment.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
16.3	**“Perform Root Cause Analysis on Security Vulnerabilities”**	Software	Protect	IG2	When significant vulnerabilities are found, look past the individual bug to the reason it was introduced: a missing standard, a flawed library, a design pattern, a gap in testing or training. Use those findings to fix classes of weakness rather than single instances.
16.4	**“Establish and Manage an Inventory of Third-Party Software Components”**	Software	Identify	IG2	Maintain an up-to-date inventory, often called a software bill of materials (SBOM), of the open-source and commercial components, libraries and frameworks used in each application, including those planned for use, with the risk each brings. Check it at least monthly for new versions, vulnerabilities and end of support.
16.5	**“Use Up-to-Date and Trusted Third-Party Software Components”**	Software	Protect	IG2	Build on well-maintained, widely used components and frameworks with a good security record, obtained from trustworthy sources, and keep them updated. Where a component's origin or quality is uncertain, assess it for vulnerabilities before use.
16.6	**“Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities”**	Documentation	Govern	IG2	Adopt a documented way of rating application vulnerabilities by severity so that fixes are prioritised consistently, and set the minimum security bar a release must meet before it goes live. Review the rating system and process at least yearly.
16.7	**“Use Standard Hardening Configuration Templates for Application Infrastructure”**	Software	Protect	IG2	Harden the platforms applications run on, such as servers, databases, web and application servers, containers, PaaS and SaaS settings, using recognised industry baselines, and make sure application code and deployment scripts do not undo that hardening.
16.8	**“Separate Production and Non-Production Systems”**	Network	Protect	IG2	Keep development, test and other non-production environments separate from production, with different access, credentials and data controls, so that work in progress cannot affect live systems or expose live data.
16.9	**“Train Developers in Application Security Concepts and Secure Coding”**	Users	Protect	IG2	Give everyone who builds software, including developers, testers, DevOps engineers and contractors, at least yearly training in secure coding relevant to their languages, frameworks and responsibilities, delivered in a way that builds a security-minded engineering culture.
16.10	**“Apply Secure Design Principles in Application Architectures”**	Software	Protect	IG2	Design applications using established security principles: least privilege, complete mediation of every request, treating all input as untrusted and validating it for type, length, range and format, failing safely, and keeping the attack surface of the application and its infrastructure small by removing unused services, files, ports and default accounts.
16.11	**“Leverage Vetted Modules or Services for Application Security Components”**	Software	Identify	IG2	Rely on proven, maintained platform services and libraries for security-critical functions such as identity, authentication, authorisation, cryptography, secrets management and audit logging, instead of writing them from scratch, and use only current, widely reviewed cryptographic algorithms.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
16.12	**“Implement Code-Level Security Checks”**	Software	Protect	IG3	Use automated static and dynamic analysis within the development life cycle to check that secure coding standards are being met, with results acted on before release.
16.13	**“Conduct Application Penetration Testing”**	Software	Detect	IG3	Have skilled testers manually probe applications, especially critical ones, both with and without valid credentials, to find business-logic flaws, authorisation gaps and chained weaknesses that automated tools miss.
16.14	**“Conduct Threat Modeling”**	Software	Protect	IG3	Before building or significantly changing an application, analyse its design in a structured way to identify how it could be attacked at each entry point and privilege level, and decide on mitigations while they are still cheap to implement. Threat modelling is carried out by people trained in the technique.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
16.1	**1.** Write a short SDLC standard that defines security activities at each phase: requirements, design, build, test, release and operate, with mandatory gates for higher-risk applications. **2.** Adopt a reference model to structure it, such as OWASP SAMM, the NIST Secure Software Development Framework (SP 800-218) or OWASP ASVS for requirements. **3.** Apply it to in-house teams, contractors and outsourced developers through contract terms (see 15.4), and to low-code, scripts and ERP customisation, not only to product code. **4.** Review the standard annually, recording changes driven by incidents, new technologies (for example AI-assisted coding) or regulation.	• Approved SDLC standard with version and review date. • Mapping of SDLC activities to release gates in the delivery pipeline. • Contract clauses applying the SDLC to outsourced developers.
16.2	**1.** Publish a vulnerability disclosure policy and a contact route (for example a security.txt file and a monitored mailbox) stating scope, safe-harbour intent and expected response times. **2.** Log every report, from scanners, pen tests, bug bounty, customers or researchers, in one tracker with severity, owner, status and dates of receipt, triage, fix and verification. **3.** Set remediation targets by severity and track the time to identify, analyse and fix; escalate breaches of target. **4.** Define how and when customers and, where needed, CERT-In are informed of vulnerabilities in products the organisation supplies.	• Published vulnerability disclosure policy and security contact. • Vulnerability tracker extract with severity and timestamps. • Periodic report of time-to-remediate against target.

Safeguard	Practical steps	Evidence
16.3	**1.** Require a short root-cause record for every critical and high vulnerability and for recurring medium ones, classified using CWE categories. **2.** Review root causes quarterly to spot patterns (for example repeated injection flaws from one framework or missing authorisation checks in one service). **3.** Turn findings into systemic fixes: new linting or SAST rules, a shared secure component, updated coding standards, targeted training or a new test case. **4.** Track whether recurrence falls after each systemic fix.	• Root-cause records linked to vulnerability tickets. • Quarterly trend analysis by CWE. • Change records for standards, rules or components that resulted.
16.4	**1.** Generate an SBOM per application in a standard format (SPDX or CycloneDX) automatically from the build, including transitive dependencies. **2.** Store SBOMs centrally and link them to the application inventory (2.1) and owners. **3.** Run a monthly or continuous check of all components against vulnerability databases and support status, and record the risk of each component (licence, maintenance health, known vulnerabilities). **4.** Record components approved for future use so new projects choose from an assessed list.	• SBOMs for a sample of applications produced from current builds. • Monthly or continuous component review records. • List of approved and prohibited components.
16.5	**1.** Pull dependencies only through approved registries or an internal proxy or artefact repository that blocks known-malicious and unapproved packages. **2.** Pin versions, verify checksums or signatures, and protect against dependency confusion and typosquatting. **3.** Use automated dependency-update tooling with tests so that security patches are adopted within the severity targets set under 16.6. **4.** Assess new or niche components for maintenance activity, known vulnerabilities and licence before approval.	• Package manager configuration pointing to approved sources. • Dependency-update pull requests and merge history. • Component approval records for new dependencies.
16.6	**1.** Base severity on a recognised scheme such as CVSS, adjusted for exploitability and business context (data exposed, internet-facing, compensating controls); consider EPSS or known-exploited lists for prioritisation. **2.** Set remediation targets per severity (for example critical within 7 days, high within 30) and the release rule (for example no open critical or high in internet-facing releases without approved exception). **3.** Define an exception process with risk owner sign-off and expiry. **4.** Review ratings, targets and exceptions annually.	• Severity rating standard with remediation targets and release criteria. • Release records showing gate decisions. • Exception register with approvals and expiry dates.

Safeguard	Practical steps	Evidence
16.7	**1.** Select baselines for each infrastructure component, such as CIS Benchmarks for operating systems, databases, web servers, Kubernetes and cloud accounts. **2.** Encode baselines as infrastructure-as-code and hardened base images, and scan templates and running environments for drift. **3.** Prevent applications from requiring weakening changes (running as root, disabling TLS checks, opening admin ports) without an approved exception. **4.** Include SaaS and PaaS security settings (tenant configuration, storage access, logging) in the baseline.	• Approved hardening baselines per platform. • IaC or configuration scan results showing compliance. • Exception records for deviations required by applications.
16.8	**1.** Separate environments by network segment, cloud account or subscription, and identity, with no shared credentials or secrets. **2.** Restrict production access to operations or release roles; developers access production only through approved, logged break-glass procedures. **3.** Prohibit live personal data in non-production unless masked or synthesised, consistent with DPDP purpose limitation. **4.** Promote code only through the pipeline, never by direct copy from development to production.	• Architecture or network diagrams showing environment separation. • Access lists for production versus non-production. • Test-data management procedure and masking evidence.
16.9	**1.** Provide core training on common weakness classes (OWASP Top 10, API Security Top 10, CWE Top 25) tailored to the stack in use. **2.** Add practical labs, secure code review sessions and capture-the-flag exercises, and use real findings from 16.3 as material. **3.** Appoint security champions in each team to coach peers and act as a link to the security function. **4.** Track completion yearly and on joining, including for outsourced developers.	• Developer training curriculum mapped to the technology stack. • Completion records for staff and contractors. • Security champion roster and activity records.
16.10	**1.** Publish secure design principles and patterns in the SDLC, with examples for the frameworks used. **2.** Require server-side authorisation checks on every operation and object, and central input validation and output encoding. **3.** Include a design review for new applications and major changes that checks these principles. **4.** Strip defaults from deployed components: sample apps, debug endpoints, default accounts and unused ports.	• Secure design principles document. • Design review records for a sample of projects. • Scan or configuration evidence of removed defaults and debug features.
16.11	**1.** Specify approved components: central identity provider (OIDC or SAML), standard authorisation library, platform key-management service and secrets vault, standard logging library. **2.** Ban custom cryptography and deprecated algorithms (for example MD5, SHA-1 for signatures, DES, RC4) through standards and code scanning rules. **3.** Provide reusable internal modules or templates that wrap these services for developers.	• Approved security component list. • Code scan results showing no prohibited algorithms or hard-coded secrets. • Architecture records showing use of the central identity and key-management services.

Safeguard	Practical steps	Evidence
16.12	**1.** Run SAST and secret scanning on every pull request or commit, and software composition analysis (SCA) on dependencies. **2.** Run DAST or API security testing against staging builds for web and API applications, and IaC scanning on templates. **3.** Tune rules to reduce false positives, route findings to the vulnerability tracker (16.2) and enforce the release threshold from 16.6. **4.** Track coverage: which repositories and applications are scanned and how often.	• Pipeline configuration showing SAST, SCA, secret and DAST stages. • Scan results and associated tickets for a sample of releases. • Coverage report of repositories under scanning.
16.13	**1.** Define which applications need penetration testing and how often, based on criticality, exposure and change rate (for example yearly and on major release for critical internet-facing apps). **2.** Include authenticated testing with each user role, API testing and business-logic scenarios such as payment manipulation or approval bypass. **3.** Use qualified testers, independent of the developers; regulated entities may need CERT-In empanelled auditors. **4.** Track findings to closure in the vulnerability tracker and retest to confirm fixes.	• Penetration testing schedule linked to the application inventory. • Test reports with scope, methods and findings. • Retest evidence for closed findings.
16.14	**1.** Train architects and security champions in a method such as STRIDE, attack trees or the OWASP threat modelling process, and supply a template. **2.** Model new critical applications and major changes: data-flow diagram, trust boundaries, threats per element, mitigations and residual risk. **3.** Turn mitigations into tracked requirements and test cases, and revisit the model when architecture changes. **4.** Include AI and LLM components where used, covering prompt injection and data leakage.	• Threat models for a sample of critical applications. • Requirements or tickets created from mitigations. • Training records for people performing threat modelling.

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
No IG1 Safeguards. IG1 enterprises that buy rather than build software rely on Controls 2 (supported software), 7 (patching) and 15 (provider contracts). If they commission a website or app, they should still ask the developer to follow a basic secure-development standard and to fix reported vulnerabilities, as a step towards IG2.	IG2 enterprises must implement 16.1 to 16.11: a documented secure SDLC (16.1); a vulnerability intake and handling process with an external reporting route (16.2); root-cause analysis (16.3); a component inventory or SBOM reviewed at least monthly (16.4); trusted, up-to-date components (16.5); a severity rating and release threshold (16.6); hardened application infrastructure (16.7); separated production and non-production (16.8); annual developer security training (16.9); secure design principles (16.10); and vetted modules for security functions (16.11). A 15-developer start-up can meet this with a two-page SDLC, open-source scanners in its pipeline, a security.txt file, a CVSS-based tracker and separate cloud accounts per environment.	IG3 adds verification: static and dynamic analysis in the life cycle (16.12), manual application penetration testing with and without credentials (16.13) and structured threat modelling by trained people (16.14). These suit enterprises with critical customer-facing applications, regulated data or software products sold to others.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 16.1 → 8.25 Secure development life cycle; 8.26 Application security requirements; 8.30 Outsourced development; 5.8 Information security in project management

- 16.2 → 8.8 Management of technical vulnerabilities; 5.24 Information security incident management planning and preparation; 5.5 Contact with authorities; 6.8 Information security event reporting
- 16.3 → 8.8; 5.27 Learning from information security incidents; clause 10.2 Nonconformity and corrective action
- 16.4 → 5.21 Managing information security in the ICT supply chain; 5.9 Inventory of information and other associated assets; 8.8
- 16.5 → 5.21; 8.19 Installation of software on operational systems; 8.28 Secure coding
- 16.6 → 8.8; 8.29 Security testing in development and acceptance; clause 6.1.2 Information security risk assessment
- 16.7 → 8.9 Configuration management; 8.27 Secure system architecture and engineering principles; 5.23 Information security for use of cloud services
- 16.8 → 8.31 Separation of development, test and production environments; 8.33 Test information; 8.4 Access to source code
- 16.9 → 6.3 Information security awareness, education and training; 8.28 Secure coding; clause 7.2 Competence
- 16.10 → 8.27 Secure system architecture and engineering principles; 8.26; 8.28
- 16.11 → 8.24 Use of cryptography; 8.5 Secure authentication; 8.15 Logging; 8.27
- 16.12 → 8.29 Security testing in development and acceptance; 8.28; 8.32 Change management
- 16.13 → 8.29; 8.8; 5.35 Independent review of information security
- 16.14 → 8.27; 8.26; 5.8

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0: PR.PS-06 (secure software development practices) for 16.1, 16.9–16.12 and 16.14; ID.RA-08 (processes for receiving, analysing and responding to vulnerability disclosures) for 16.2; ID.RA-01 (vulnerabilities identified) for 16.12–16.13; ID.AM-02 (software inventories) and GV.SC-09 for 16.4–16.5; PR.PS-01 (configuration management) for 16.7; PR.IR-01 (networks and environments protected) for 16.8; ID.IM-02 and ID.IM-03 (improvements from tests and operations) for 16.3 (Srida IT mapping)
- NIST SP 800-218 Secure Software Development Framework (SSDF) practice groups PO, PS, PW and RV align closely with this Control
- NIST SP 800-53 Rev. 5: SA-3, SA-8, SA-11, SA-15, SA-17 (development process, design principles, developer testing), SR-4 and SR-11 (provenance, component authenticity), RA-5 and RA-5(11) (vulnerability monitoring and public disclosure programme), CM-4 and CM-7
- OWASP resources as open references: SAMM, ASVS, Top 10, API Security Top 10 and the Threat Modelling Cheat Sheet

F India Regulatory Touchpoints

- RBI Master Direction on IT Governance, Risk, Controls and Assurance Practices (2023): secure SDLC, application security testing, source-code review or escrow, and separation of environments for regulated entities.
- SEBI CSCRF (2024): application security testing and software bill of materials expectations for regulated entities, with VAPT by CERT-In empanelled auditors for certain categories.
- CERT-In: technical guidelines on SBOM (2024) and the vulnerability-reporting route for products; CERT-In empanelled auditors are often required for application security audits of government and regulated systems.
- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6: reasonable security safeguards, including measures such as encryption, access control and logging that secure applications must implement, and protection of personal data in test environments.

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Web applications and APIs are among the most frequently attacked surfaces of any organisation. Injection flaws, broken access control that lets one customer see another's records, weak session handling and exposed APIs lead directly to data theft and fraud. Supply-chain attacks through compromised or malicious open-source packages, and incidents in which a widely used library contained a critical flaw, have shown that most of an application's code is often written by someone else, and that an organisation unable to say where a component is used cannot respond quickly when one is found to be vulnerable.

Fixing a flaw after release costs many times more than avoiding it at design time, and some flaws (an architecture that trusts the client, a missing tenant boundary) can be impossible to fix without a rewrite. A disciplined SDLC, with design review, trusted components, automated checks and focused manual testing, is what moves security left and keeps the cost manageable. Root-cause analysis then stops the same weakness reappearing in every release.

India's digital economy runs on applications: UPI-connected payment apps, lending apps, e-commerce, health-tech and government-facing portals. Regulators are paying attention. RBI's IT governance directions expect a secure SDLC, source-code assurance and application security testing for regulated entities; SEBI CSCRF calls for software bill of materials and application security testing; CERT-In has issued technical guidance on SBOM; and the DPDP Act requires reasonable security safeguards to prevent personal-data breaches, which for most data fiduciaries means secure applications. Many Indian start-ups and IT services firms also build software for global clients who will ask for evidence of these practices.

I Applicability

Control 16 applies wherever the enterprise writes, commissions, customises or hosts software. A small firm whose website is built by an agency should place 16.1, 16.2 and 16.5 obligations on the agency by contract and ask for a basic scan report before go-live. Bengaluru-style SaaS start-ups will find IG2 achievable with open-source pipeline tooling and should treat 16.4 SBOMs and 16.2 disclosure handling as customer-facing requirements. IT services and outsourced development firms must show these practices to clients and should align with their clients' SDLCs under contract. ERP and low-code customisation is in scope: custom ABAP, scripts, workflows and integrations carry the same risks as product code. OT manufacturers should apply 16.7 and 16.8 to HMI, SCADA and MES applications and require secure development from integrators. Where development is fully outsourced, the enterprise remains responsible for setting requirements, reviewing evidence and owning the vulnerability tracker.

J Implementation Guidance

1. Inventory all applications and code repositories, including outsourced, low-code and ERP customisations, and assign an owner and criticality to each.
2. Write a concise secure SDLC standard based on a recognised model, with gates scaled to application criticality, and apply it to contractors by contract.
3. Publish a vulnerability disclosure policy and set up one tracker for all application vulnerabilities, with a CVSS-based severity standard, remediation targets and a release threshold.
4. Separate production from non-production by account, network and identity, and adopt test-data masking.
5. Harden application infrastructure with recognised baselines encoded in infrastructure-as-code and hardened images, scanned for drift.
6. Introduce SBOM generation and SCA in the build, route dependencies through an approved repository and automate dependency updates.
7. Standardise security building blocks: central identity provider, secrets vault, key-management service, logging library, approved cryptography.
8. Train developers yearly in secure coding for their stack and appoint security champions.
9. Add SAST, secret scanning, IaC scanning and DAST to pipelines, and enforce the release threshold (IG3).
0. Perform threat modelling for new critical applications and major changes, and schedule penetration testing by criticality, feeding findings into root-cause analysis and training (IG3).

K Tools and Automation

- Source-code management and CI/CD platform with branch protection and mandatory review: the backbone where security gates are enforced.
- Static application security testing (SAST) and secret scanning, including open-source options such as Semgrep and gitleaks: find coding flaws and leaked credentials early.
- Software composition analysis (SCA) and SBOM generators, including open-source options such as OWASP Dependency-Track, Syft and Grype: maintain component inventories and match them against vulnerability data.
- Dynamic application and API security testing (DAST), such as OWASP ZAP: test running applications in staging.
- Infrastructure-as-code and container image scanners, such as Trivy or Checkov: check templates and images against hardening baselines.
- Artefact repository or package proxy: controls where dependencies come from and blocks malicious packages.

- Vulnerability tracker or issue system with severity fields and SLA reporting; threat modelling tools such as OWASP Threat Dragon.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
CTO or head of engineering	Owns the secure SDLC, ensures teams follow it and funds tooling and training.
CISO or application security lead	Sets security requirements, severity standard and release thresholds; reviews threat models and pen test results; owns the disclosure policy.
Developers and DevOps engineers	Follow secure coding standards, fix findings within targets and maintain pipelines and infrastructure-as-code.
Security champions	Coach their team, triage tool findings and participate in threat modelling and root-cause reviews.
Product or application owner	Accepts residual risk, approves exceptions and prioritises remediation in the backlog.
QA and test team	Include security test cases and verify fixes.
Procurement and legal	Apply SDLC and vulnerability-handling obligations to outsourced developers and software suppliers.
Independent penetration testers	Perform manual testing with appropriate independence and qualifications.

M Documentation and Records

- Secure SDLC standard and secure coding guidelines per language or framework.
- Vulnerability disclosure policy and internal vulnerability handling procedure.
- Severity rating standard with remediation targets, release thresholds and exception process.
- Application and repository inventory with criticality and owners.
- SBOMs and approved component list.
- Hardening baselines for application infrastructure.
- Environment separation design and test-data management procedure.
- Secure design principles and approved security component list.
- Developer training curriculum and records.
- Threat models, penetration test reports and root-cause analysis records.

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 22-2. Assessment testing procedures, Control 16

Test ID	Method	Testing procedure	Result
TP-C16-01	**EXAMINE**	16.1: Examine the secure SDLC standard. Confirm it addresses design standards, secure coding, developer training, vulnerability management, third-party code and security testing; that it applies to outsourced and low-code development; and that it was reviewed within the last twelve months or after the latest significant change.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-02	**SAMPLE**	16.1: Sample five releases of critical applications in the period and trace each through the SDLC gates (requirements, design review, testing, release approval). Record any gate that was skipped without an approved exception.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-03	**RE-PERFORM**	16.2: Locate the external vulnerability reporting route (website, security.txt or published policy) and confirm it is current. Submit a benign test report by agreement with management and measure time to acknowledgement. Examine the procedure for intake, assignment, remediation and retest.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C16-04	SAMPLE	16.2: Sample 20 vulnerabilities closed in the period across sources (scanner, pen test, external report) and confirm each has a severity, owner and timestamps for receipt, triage, fix and verification, and that time-to-remediate metrics are reported.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-05	EXAMINE	16.3: For a sample of critical and high vulnerabilities, examine root-cause records. Confirm causes are classified (for example by CWE), trends are reviewed periodically and at least one systemic action (standard, rule, component or training change) resulted in the period.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-06	INSPECT	16.4: For a sample of applications, inspect the SBOM and confirm it was generated from a current build, includes transitive dependencies and records component risk. Examine evidence that the component list is evaluated at least monthly for updates, vulnerabilities and end of support.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-07	RE-PERFORM	16.4: Select one application, independently generate a component list from its source or build with an SCA or SBOM tool, and compare it with the recorded SBOM. Report missing components.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-08	INSPECT	16.5: Inspect package-manager and build configuration to confirm dependencies are drawn from approved sources, versions are pinned and integrity is verified. Sample dependencies with known high or critical vulnerabilities and confirm they were updated within the targets set by the severity standard.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-09	EXAMINE	16.6: Examine the severity rating standard and confirm it defines ratings, remediation targets, a minimum release threshold and an exception process, and was reviewed in the last year. Sample release decisions and exceptions to confirm the threshold is enforced and exceptions are approved and time-bound.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-10	INSPECT	16.7: Inspect configuration scan results for servers, databases, web servers, containers and cloud or SaaS settings supporting a sample of applications against the adopted hardening baselines. Identify deviations introduced by application requirements and confirm they are approved.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-11	INSPECT	16.8: Inspect environment architecture and access lists. Confirm production and non-production are separated by network or account and identity, that developers lack standing production access, and that secrets differ between environments. Sample non-production databases for unmasked personal data.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-12	SAMPLE	16.9: Sample developers, testers, DevOps engineers and contractor developers and confirm each completed secure-coding training relevant to their stack within the last twelve months or since joining. Examine the curriculum for relevance to the languages and frameworks used.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-13	EXAMINE	16.10: Examine the secure design principles and a sample of design review records. Inspect one critical application for server-side authorisation on sampled functions, input validation and removed default accounts, debug endpoints and unused services.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-14	INSPECT	16.11: Inspect the approved security component list and a sample of applications to confirm authentication uses the central identity service, secrets are held in the vault or key-management service, logging uses the standard library and no prohibited or home-grown cryptography is present (supported by a code search).	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C16-15	**INSPECT**	16.12: Inspect pipeline definitions for a sample of repositories to confirm SAST, secret scanning, SCA and, for web and API applications, DAST stages run on each change or release. Confirm findings reach the tracker and that the release threshold blocks or requires an exception. Examine the coverage report for unscanned repositories.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-16	**EXAMINE**	16.13: Examine the penetration testing schedule against the application inventory and confirm critical applications were tested within the required interval and after major change. Examine reports for authenticated and unauthenticated testing and business-logic scope, tester independence and retest evidence for closed findings.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-17	**EXAMINE**	16.14: Sample new critical applications or major changes in the period and examine their threat models for data flows, trust boundaries, threats and mitigations. Trace mitigations to backlog items or tests and confirm the people performing the modelling were trained.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C16-18	**INTERVIEW**	16.1, 16.9 and 16.14: Interview two developers and one architect about how security is considered in their daily work, what they learned in training and when a threat model is required; compare answers with the documented process.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Base the population on the application inventory, weighting samples towards critical and internet-facing applications. For organisations with up to ten applications, include all critical applications and at least one non-critical. For larger estates, sample five to eight applications, including at least one outsourced build, one API or mobile application and, where present, one ERP customisation or low-code application. For vulnerability records, sample 20 to 25 closed and 10 open items across sources and severities over the last twelve months. Sample releases from the same period. Record populations, selections and exceptions in WP-C16.

P Interview Questions

Interviewee	Question
Head of engineering	How does a team know which security steps are mandatory for a given release, and who can waive them?
Developer	What happens when the scanner flags a high-severity finding the day before a release?
Application security lead	Show me the last root-cause review. What did you change as a result?
DevOps engineer	Where do your dependencies come from, and how would you know within a day if a library you use had a critical vulnerability announced?
Product owner	When did you last accept a security risk to meet a deadline, and when does that acceptance expire?
Outsourced development partner	Which of our security requirements are in your contract, and how do you evidence them?

Q Technical and Process Verification

- A secure SDLC exists, is current and is applied to sampled releases including outsourced work.
- Vulnerabilities from all sources are tracked with severity and timing against targets.
- SBOMs are current and reconcile to independently generated component lists.
- Environments are separated and test data is protected.
- Developers are trained and security components are standardised.
- For IG3, automated testing, penetration testing and threat modelling are performed and drive fixes.

R Expected Evidence

- SDLC standard, secure coding guidelines and design principles.

- Published vulnerability disclosure policy and tracker extracts.
- Severity standard, release gate records and exception register.
- SBOMs and SCA reports.
- Hardening baseline and configuration scan reports.
- Environment architecture diagrams and access lists.
- Developer training records and champion roster.
- Pipeline configurations and scan results.
- Penetration test reports, threat models and root-cause analysis records.

S Evaluation Criteria

Implemented

- A secure SDLC with severity-based release gates is applied to all in-scope development, including outsourced and low-code work.
- Vulnerability intake, tracking and root-cause analysis operate with measured timeliness.
- SBOMs, trusted components, hardened platforms, separated environments, trained developers and standard security modules are in place (IG2).
- Automated analysis, penetration testing and threat modelling are performed and acted on (IG3).

Partially implemented

- An SDLC is documented but not enforced in pipelines, or excludes outsourced or ERP development.
- Scanners run but findings are not tracked to remediation targets, or SBOMs are incomplete or stale.
- Penetration testing occurs but is unauthenticated only or findings are not retested.

Not implemented

- No defined secure development process; security depends on individual developers.
- No way for outsiders to report vulnerabilities and no central tracking.
- Production and development share credentials, networks or live personal data.

T Common Gaps and Findings

- Condition: the customer portal's SBOM was last generated nine months ago. Criteria: 16.4 expects at least monthly evaluation. Effect: the organisation could not tell whether a newly disclosed critical library flaw affected it.
- Condition: no public vulnerability reporting route; a researcher's report sat in a general sales inbox for six weeks. Criteria: 16.2. Effect: avoidable exposure and reputational risk.
- Condition: the UAT database is a nightly copy of production containing unmasked customer KYC data. Criteria: 16.8 and DPDP reasonable safeguards. Effect: personal data exposed to developers and contractors without need.
- Condition: the outsourced mobile app team is not covered by SDLC or training obligations. Criteria: 16.1 and 16.9. Effect: inconsistent security quality in a customer-facing channel.
- Condition: penetration tests are unauthenticated only. Criteria: 16.13. Effect: authorisation flaws allowing one customer to view another's loan records were missed.
- Condition: the same insecure direct object reference flaw was fixed in three releases. Criteria: 16.3. Effect: no systemic fix; the weakness keeps recurring.

U Remediation Guidance

- Automate SBOM generation on every build and connect it to a component-monitoring platform with alerts for new critical vulnerabilities.
- Publish a vulnerability disclosure policy and security.txt, route reports to a monitored security mailbox and log them in the tracker.
- Introduce masked or synthetic test data and remove production copies from non-production within an agreed period.
- Amend outsourced development contracts to require compliance with the SDLC, training and evidence of scanning, and include partners in champion forums.
- Commission authenticated, role-based penetration testing of critical applications and retest fixes.
- Run a root-cause review on recurring flaws and implement a shared authorisation component with tests and a SAST rule.

V Monitoring Metrics

- Mean and 90th-percentile time to remediate application vulnerabilities by severity, against targets.

- Percentage of active repositories with SAST, secret scanning and SCA in the pipeline; target 100 per cent for critical applications.
- Percentage of applications with an SBOM refreshed within the last 30 days.
- Percentage of releases of critical applications passing the release threshold without exception.
- Rate of recurrence of the top five CWE categories quarter on quarter.
- Percentage of developers, including contractors, with secure-coding training in the last twelve months.

W Related Controls and Maturity Indicators

- 2.1–2.2 (software inventory and support status that 16.4 extends to components)
- 3.11–3.12 (encryption and segmentation of sensitive data used by applications)
- 4.1 and 4.2 (secure configuration that 16.7 applies to application platforms)
- 6.3–6.5 and 6.8 (authentication and role-based access applications should consume, see 16.11)
- 7.1–7.7 (vulnerability management that 16.2 and 16.6 specialise for code)
- 8.2 and 8.5 (application audit logging)
- 13.10 and 12.2 (application-layer filtering and network segmentation)
- 14.9 (role-specific training, of which 16.9 is a form)
- 15.4 (contracts for outsourced development)
- 18.2–18.3 (penetration testing at enterprise level)

Initial	Defined	Managed	Optimised
Security depends on individual developers; no documented SDLC; vulnerabilities fixed ad hoc when someone reports them.	A secure SDLC, severity standard and disclosure route exist; environments are separated; developers receive annual training; SBOMs are produced for key applications.	Pipeline security checks, SBOM monitoring and release gates are enforced; vulnerabilities are tracked against targets; root-cause trends drive standards and training; critical apps are penetration tested and threat modelled.	Security is measured as an engineering quality attribute; paved-road secure components dominate; recurrence of weakness classes declines measurably; customers and regulators receive SBOM and testing evidence routinely.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A Bengaluru SaaS start-up with 120 staff, 45 of them engineers, sold an HR and payroll platform to Indian mid-market companies. A large prospective customer, itself a SEBI-regulated entity, sent a security questionnaire asking for an SBOM, a vulnerability disclosure policy, the last penetration test report and evidence of a secure SDLC. The start-up could answer only the last item, and that test had been unauthenticated.

The CTO and a newly hired application security lead drew up a 90-day plan. A four-page SDLC based on the NIST SSDF and OWASP SAMM was approved, with gates proportionate to service criticality. Semgrep, gitleaks and an SCA scanner were added to every pull request in the CI pipeline; Syft produced CycloneDX SBOMs on each build, which were loaded into an open-source dependency-tracking platform that alerted on new critical vulnerabilities. A security.txt file and disclosure policy were published, and all findings were moved into one tracker with CVSS-based severity and targets of 7 days for critical and 30 for high, with no open criticals allowed in a production release.

Engineering found that the staging database held a full copy of production payroll data. It was replaced with synthetic data generated from schema rules, and production access for developers was replaced with a logged break-glass process. Each squad nominated a security champion, and all engineers, including two contracted mobile developers, completed a stack-specific secure-coding course.

An authenticated penetration test then found that changing an employee ID in an API call exposed another tenant's payslips. The fix was quick, but the root-cause review found the same pattern in four services; the team built a shared authorisation middleware with tests and a Semgrep rule to block direct object lookups without it. Threat modelling became mandatory for new services.

The assessor rated 16.1 to 16.12 Implemented, 16.13 Implemented after retest, and 16.14 Partially implemented, because legacy services had not yet been modelled.

WP-C16: use the workpaper format shown in Appendix H.

CHAPTER 23 · CIS CONTROL 17

Incident Response Management

CIS CONTROL 17 · 9 SAFEGUARDS · 3 IN IG1

Incident Response Management

CIS Controls v8.1 · titles quoted verbatim | WP-C17

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 17 — Incident Response Management

Control 17 is about being ready before something goes wrong and then handling it well when it does. It asks for named people to lead incident handling, an up-to-date list of who to notify, a simple way for every employee to report problems, a documented response plan with roles and communication arrangements, regular exercises, honest post-incident reviews and clear thresholds that say when an event becomes an incident. The Control is heavily process and people-centred: six of its nine Safeguards concern users and documentation rather than technology. Its value is in speed and coordination. An organisation with good protective controls but no response plan will still lose days arguing about who is in charge, whether to call the insurer, what to tell customers and whether the regulator must be told. In India those questions carry hard deadlines, notably the CERT-In six-hour reporting window and the personal data breach intimation duties under the DPDP Act and Rules, so preparation is a compliance necessity as much as a security one.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 23-1. Safeguards of CIS Control 17, Incident Response Management

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
17.1	**“Designate Personnel to Manage Incident Handling”**	Users	Respond	IG1	A named individual is accountable for running incident handling, with at least one named deputy who can take over when the primary is unavailable. The role may be filled by staff, an external provider or a mix, but where a provider is used an internal person oversees it. The appointment is revisited every year and whenever the organisation changes materially.
17.2	**“Establish and Maintain Contact Information for Reporting Security Incidents”**	Documentation	Govern	IG1	The organisation holds an up-to-date list of everyone it may need to tell, or call on, when a security incident happens: internal staff, providers, insurers, regulators and authorities, law enforcement and information-sharing groups. The list is checked at least once a year.
17.3	**“Establish and Maintain an Enterprise Process for Reporting Incidents”**	Documentation	Govern	IG1	Every member of the workforce knows how to report a suspected security incident: what to report, to whom, how and how quickly, and what details to give. The process is written down, easy for all staff to find and reviewed every year.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
17.4	**“Establish and Maintain an Incident Response Process”**	Documentation	Govern	IG2	A documented incident response process sets out who does what, which legal, regulatory and contractual obligations apply, and how communication will be handled during and after an incident. It is reviewed at least annually and after significant change.
17.5	**“Assign Key Roles and Responsibilities”**	Users	Respond	IG2	Specific responsibilities in incident response are assigned to named people or teams, including responders, analysts, decision-makers and outside parties, so that nobody has to work out who does what during a crisis. Assignments are reviewed every year and after significant change.
17.6	**“Define Mechanisms for Communicating During Incident Response”**	Users	Respond	IG2	The organisation decides in advance which primary and backup channels it will use to coordinate and report during an incident, recognising that email, chat or phone systems may themselves be compromised or unavailable. The choice is reviewed annually.
17.7	**“Conduct Routine Incident Response Exercises”**	Users	Recover	IG2	People with incident response duties take part in planned exercises, at least once a year, that test how they communicate, make decisions and follow the workflow against realistic scenarios.
17.8	**“Conduct Post-Incident Reviews”**	Users	Recover	IG2	After incidents are closed, the organisation reviews what happened, what went well and what did not, and turns the lessons into tracked improvements so that the same incident is less likely to happen again.
17.9	**“Establish and Maintain Security Incident Thresholds”**	Documentation	Recover	IG3	The organisation defines clear thresholds that separate a routine security event from an incident, and categorises incidents (for example suspicious activity, vulnerability, weakness, data breach, privacy incident) with severity levels that drive escalation. Thresholds are reviewed annually.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
17.1	**1.** Appoint an incident manager and at least one deputy in writing, with authority to convene people, spend within an agreed limit and make containment decisions. **2.** Where an MSP, MSSP or retained incident response firm is used, name an internal owner who directs their work and signs off their reports. **3.** Record the appointments in the incident response policy and contact list, and review them each year and after restructures, resignations or new outsourcing.	• Appointment letter, policy extract or RACI naming the incident manager and deputy • Record of the last annual review of the appointment • Contract or engagement letter for any external incident response provider, with the internal owner named

Safeguard	Practical steps	Evidence
17.2	**1.** Compile the list: incident team, senior management, legal, communications, key IT and cloud providers, cyber insurer and its breach hotline, retained forensic firm, CERT-In, the sector regulator, the Data Protection Board route under the DPDP Act, the local cyber crime cell and any sector CSIRT or ISAC. **2.** Record for each contact the circumstances in which they are notified, the channel to use and any deadline, so the list doubles as a notification matrix. **3.** Store copies where they remain reachable if corporate systems are down (printed, offline and on personal devices of the incident team), and verify every entry each year by actually contacting it.	• Current contact list or notification matrix with a last-verified date per entry • Record of the annual verification exercise • Evidence that an offline copy exists
17.3	**1.** Write a short reporting procedure that says what counts as reportable (phishing, lost devices, suspicious activity, misent data), the reporting channels (a phishing-report button, a mailbox, a phone number, the service desk), the time expected (for example immediately or within one hour) and the minimum details to include. **2.** Publish it on the intranet, in onboarding material and on posters or desk cards, and cover it in awareness training under Control 14. **3.** Review it annually and when channels or organisation change, and test that reports actually reach the incident manager.	• Published reporting procedure and its location • Training or onboarding material that covers reporting • Sample of staff reports received through the channel with timestamps
17.4	**1.** Write an incident response plan covering preparation, detection and analysis, containment, eradication, recovery and post-incident activity, aligned to a recognised model such as NIST SP 800-61 or ISO/IEC 27035. **2.** Include a compliance section that lists every reporting obligation with its trigger, recipient and deadline: CERT-In within six hours, sector regulator timelines, DPDP breach intimation to the Data Protection Board and affected Data Principals, contractual notifications to clients and insurer notification terms. **3.** Add playbooks for the most likely scenarios (ransomware, business email compromise, account takeover, data leakage, lost device, insider misuse) and a communication plan, then obtain management approval and review annually.	• Approved incident response plan with version history • Regulatory and contractual notification register within the plan • Scenario playbooks
17.5	**1.** Define the roles needed: incident manager, technical lead, forensic analyst, IT operations, legal counsel, privacy or DPO function, communications, HR, executive sponsor, and named external parties such as the MDR provider, forensic firm and cloud providers. **2.** Assign each role to a named person with a deputy, and record it in a RACI that is part of the incident response plan. **3.** Confirm that third parties know their role through contract clauses or engagement letters, and review the assignments annually.	• RACI or role table with named holders and deputies • Contract clauses defining third-party incident roles • Review record

Safeguard	Practical steps	Evidence
17.6	**1.** Choose a primary channel and at least one out-of-band backup that does not depend on the corporate identity system or network, for example a separately hosted secure messaging group, a conference bridge and a phone tree. **2.** Prepare templates for internal updates, customer notices, regulator notifications and Data Principal intimations, so that wording is not drafted from scratch under pressure. **3.** Test the backup channel during exercises and review the arrangements annually.	• Communication section of the plan naming primary and backup channels • Notification templates • Exercise record showing the backup channel was used
17.7	**1.** Plan an annual exercise programme: at least one tabletop exercise for management and the incident team, and where possible a technical drill for responders. **2.** Base scenarios on realistic threats to the organisation and include the regulatory clock, for example requiring the team to prepare a CERT-In report within six hours of detection. **3.** Record participants, observations and actions, and track the actions to closure.	• Exercise plan and scenario document • Attendance list and exercise report • Action tracker from the exercise
17.8	**1.** Set a rule for which incidents require a formal review (for example all high-severity incidents and every reportable incident) and a deadline, such as within two weeks of closure. **2.** Run a blameless review covering timeline, root cause, detection and response performance, and whether notification deadlines were met. **3.** Record improvement actions with owners and due dates, and feed them into risk, control and training updates.	• Post-incident review reports • Improvement action register with status • Evidence that actions changed controls, rules or procedures
17.9	**1.** Write event and incident definitions and a severity matrix based on impact to confidentiality, integrity, availability, personal data, customers and regulatory exposure. **2.** Map the categories to reporting triggers, for example which incident types fall within the CERT-In list of reportable incidents and which involve personal data and therefore engage DPDP breach intimation. **3.** Use the thresholds in SOC triage (Control 13) and review them each year against actual incidents.	• Incident classification and severity matrix • Mapping of categories to reporting obligations • Sample incident tickets showing classification applied

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
IG1 has three Safeguards: a named incident handler with a backup (17.1), a maintained contact list for incident notification (17.2) and a documented way for staff to report incidents (17.3). For a 40-person firm this can be a single page: the partner and office manager named as incident lead and deputy, a contact list including the IT provider, insurer, CERT-In and the bank, and a rule that staff report anything suspicious to a named mailbox or phone number immediately. Even at IG1, Indian body corporates fall within the CERT-In Directions, so the contact list and reporting procedure should make the six-hour window visible.	IG2 adds five Safeguards that make response a managed capability: a documented incident response process covering roles, compliance requirements and communications (17.4), assigned responsibilities including third parties (17.5), primary and backup communication mechanisms (17.6), routine exercises at least annually (17.7) and post-incident reviews (17.8). Most mid-sized Indian enterprises, and any that process significant volumes of personal data, should treat IG2 as the realistic target for this Control.	IG3 adds one Safeguard: defined thresholds that distinguish events from incidents and categorise incident types (17.9). This matters for enterprises with high alert volumes and multiple regulators, where consistent classification decides which incidents are escalated and which reporting clocks start. IG3 enterprises are also expected to apply the IG2 Safeguards with more rigour, for example several exercises a year, technical drills and independent review of the plan.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 17.1 → 5.24 Information security incident management planning and preparation; 5.2 Information security roles and responsibilities
- 17.2 → 5.5 Contact with authorities; 5.6 Contact with special interest groups; 5.24
- 17.3 → 6.8 Information security event reporting
- 17.4 → 5.24; 5.26 Response to information security incidents; 5.31 Legal, statutory, regulatory and contractual requirements
- 17.5 → 5.2 Information security roles and responsibilities; 5.24
- 17.6 → 5.24; 5.29 Information security during disruption; clause 7.4 Communication
- 17.7 → 5.24; 5.30 ICT readiness for business continuity; 6.3 Information security awareness, education and training
- 17.8 → 5.27 Learning from information security incidents; 5.28 Collection of evidence; clause 10.2 Nonconformity and corrective action
- 17.9 → 5.25 Assessment and decision on information security events

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0 (Srida IT mapping): RS.MA-01 to RS.MA-05 incident management (17.1, 17.4, 17.5, 17.9); RS.CO-02 and RS.CO-03 incident reporting and information sharing (17.2, 17.6); DE.AE-08 incident declaration criteria (17.9); ID.IM-02 and ID.IM-04 improvement from exercises and maintained response plans (17.7, 17.8); GV.RR-02 roles (17.1, 17.5)
- NIST SP 800-53 Rev. 5: IR-1 to IR-8 (policy, training, testing, handling, monitoring, reporting, assistance and the response plan)
- NIST SP 800-61 (incident handling guide) and ISO/IEC 27035 series as reference models for the response life cycle

F India Regulatory Touchpoints

- CERT-In Directions of 28 April 2022 under section 70B(6) of the IT Act: report the listed types of cyber incident to CERT-In within six hours of noticing them, designate a point of contact to liaise with CERT-In, and provide logs and information on request. The incident classification in 17.9 should map to the CERT-In list of reportable incidents
- DPDP Act 2023 s.8(6) and DPDP Rules 2025 r.7: on a personal data breach, the Data Fiduciary intimates each affected Data Principal without delay, and the Data Protection Board without delay with a detailed report generally within 72 hours of becoming aware; s.8(5) and r.6 require reasonable security safeguards, including breach detection and response. Commencement of these provisions is phased
- Sector regulators: RBI directions for banks and NBFCs, SEBI CSCRF (2024) for regulated entities and IRDAI guidelines for insurers each set incident reporting timelines (commonly within a few hours) and crisis management plan expectations in addition to CERT-In
- Critical information infrastructure: entities whose systems are notified as protected systems also have reporting and coordination duties towards NCIIPC

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Protective controls will fail at some point; a phishing email gets through, a supplier is breached, a misconfigured storage bucket is found. What separates a contained event from a business crisis is usually the response. Without designated leaders and a plan, technical staff often re-image the affected machine and move on, destroying evidence and leaving the attacker's other footholds in place. Without a known reporting route, staff sit on suspicious emails or lost laptops for days. Without pre-agreed communication channels, the incident team discovers mid-crisis that email and chat are in the hands of the attacker. Each of these gaps lengthens the time an adversary has inside the environment and increases the eventual cost.

A well-run response also produces learning. Post-incident reviews and exercises reveal weak detection, slow escalation and unclear decisions, and turn them into improvements in Controls 8, 13 and 14. Organisations that skip this step face the same incident repeatedly.

The India angle is direct. The CERT-In Directions of April 2022 require specified cyber incidents to be reported within six hours of being noticed, and require each service provider, intermediary, data centre and body corporate to designate a point of contact for CERT-In. The DPDP Act 2023 requires a Data Fiduciary to intimate the Data Protection Board and each affected Data Principal of a personal data breach (s.8(6)), and the DPDP Rules 2025 (r.7) set out the content and timing, including a detailed report to the Board within 72 hours. Sector regulators add their own reporting windows for banks, NBFCs, securities market entities and insurers. Meeting several overlapping clocks with different recipients and content is only possible with a plan that has been rehearsed.

I Applicability

Every organisation needs Control 17, regardless of size or architecture, because every organisation will have incidents and every Indian body corporate falls within the CERT-In Directions. A small firm meets IG1 with a page of names, numbers and a reporting rule, and can rely on its IT provider and insurer's breach response panel for technical work, provided an internal person stays in charge. SaaS- and cloud-heavy organisations must plan for incidents in systems they do not run: the plan should state how to obtain logs and support from each provider, what the contracts say about the provider's notification duties, and who holds administrative access if the identity provider is compromised. OT environments need playbooks that involve plant engineering and safety staff, since containment such as isolating a network segment may stop production or create a safety risk. Where incident response is outsourced to an MSSP, MDR or retained forensic firm, the contract should fix response times, evidence handling, data location and confidentiality, and the organisation should rehearse with the provider at least annually. Organisations acting as data processors should plan to notify their Data Fiduciary clients promptly so that those clients can meet their own DPDP duties.

J Implementation Guidance

1. Appoint the incident manager and deputy (17.1) and secure an executive sponsor who can authorise spend, shutdowns and external communication.
2. Build the notification matrix (17.2): list every internal and external party, and for each regulator or authority the trigger, deadline, channel and content. Include CERT-In, the sector regulator, the Data Protection Board route, insurers and key clients.
3. Publish a simple staff reporting procedure (17.3) with an easy channel, and cover it in onboarding and awareness training.
4. Write the incident response plan (17.4) with phases, decision rights, evidence handling, a regulatory notification section and playbooks for the five or six most likely scenarios.
5. Assign roles in a RACI (17.5), including legal, privacy, communications, HR and external providers, and align provider contracts to those roles.
6. Set up out-of-band communication (17.6) and prepare templates for CERT-In reports, regulator notices, DPDP intimations to the Board and Data Principals, and customer statements.
7. Define event and incident thresholds and a severity matrix (17.9) and wire them into SOC triage so that the reporting clock is visible from the first ticket.
8. Exercise the plan at least annually (17.7), including a scenario that tests the six-hour CERT-In report and the DPDP intimation process end to end.
9. Hold post-incident reviews (17.8) for every significant incident and every exercise, and track improvements to closure.
0. Review the whole Control annually, after major incidents and after regulatory changes, and report readiness to the board or management committee.

K Tools and Automation

- Incident case management or ticketing system: records each incident's timeline, classification, actions, evidence and notification deadlines, and supports reporting.
- SIEM and EDR consoles (Control 13): supply detection, scoping and containment capabilities such as host isolation.
- Digital forensics and incident response toolkits: open-source options such as Velociraptor for endpoint collection and triage, plus disk and memory imaging tools, used under documented chain of custody.
- Out-of-band communication platform: a secure messaging or conferencing service hosted outside the corporate tenant, with pre-created groups for the incident team.
- Tabletop exercise kits and scenario libraries: support realistic, repeatable exercises; CIS and national agencies publish free scenarios.

- Contact and notification matrix tool: a controlled document or GRC module that tracks contact verification dates and regulatory deadlines.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
Executive sponsor	Authorises major decisions, spending and external statements; chairs the crisis committee for severe incidents
Incident manager and deputy	Lead and coordinate the response, maintain the timeline and ensure notifications are made on time
Technical lead and analysts	Scope, contain, eradicate and recover; preserve evidence
Legal counsel and DPO or privacy lead	Decide on regulatory, DPDP and contractual notifications and approve their content
Communications and HR	Handle staff, customer and media communication; handle insider-related matters
CERT-In point of contact	Submits CERT-In reports and responds to CERT-In requests
External providers (MDR, forensic firm, cloud and IT providers, insurer)	Deliver the services and notifications set out in their contracts

M Documentation and Records

- Incident response policy and plan, with version history and approval
- Notification matrix and verified contact list
- Staff incident reporting procedure
- Role assignment (RACI) and provider contract extracts
- Scenario playbooks and communication templates, including CERT-In and DPDP notification templates
- Incident classification and severity matrix
- Exercise plans, reports and action trackers
- Incident register and post-incident review reports

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 23-2. Assessment testing procedures, Control 17

Test ID	Method	Testing procedure	Result
TP-C17-01	**EXAMINE**	17.1: Examine the document that appoints the incident manager and deputy. Confirm both are named, that their authority is stated, that the appointment was reviewed within the last twelve months or after the most recent organisational change, and, where a provider is used, that an internal person is named to oversee the provider.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C17-02	**INTERVIEW**	17.1: Interview the incident manager and deputy separately and ask each to describe their role, how they would be alerted out of hours and what decisions they may take without further approval. Compare their answers with the plan.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C17-03	**RE-PERFORM**	17.2: Select a sample of entries from the contact list (for example ten, including at least the insurer, CERT-In reporting channel, sector regulator, forensic provider and one internal executive) and confirm they are current by checking against official sources or by test contact. Confirm each entry shows a verification date within the last year and that an offline copy exists.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Test ID	Method	Testing procedure	Result
TP-C17-04	SAMPLE	17.3: Examine the staff reporting procedure for reporting timeframe, recipients, channels and minimum information, and confirm it is accessible to all staff. Select a sample of staff from different departments and ask them how they would report a suspected incident. Sample reports received during the period and confirm they reached the incident team promptly.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C17-05	EXAMINE	17.4: Examine the incident response plan for coverage of roles and responsibilities, response phases, evidence handling, compliance requirements and a communication plan. Confirm the compliance section lists CERT-In six-hour reporting, applicable sector regulator timelines and DPDP breach intimation to the Data Protection Board and Data Principals with correct recipients and deadlines. Confirm approval and review within the last twelve months.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C17-06	SAMPLE	17.4: Select a sample of reportable incidents from the incident register for the period. For each, compare the time of detection with the time of CERT-In, regulator and DPDP notifications, and confirm the notifications were made within the required windows with the required content. Where no reportable incidents occurred, confirm this against the SOC alert and ticket history.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C17-07	INSPECT	17.5: Inspect the RACI or role table and confirm every key role has a named holder and deputy, including legal, privacy, communications and third parties. Inspect a sample of provider contracts to confirm incident roles, response times and notification duties are specified. Confirm the assignments were reviewed within the year.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C17-08	EXAMINE	17.6: Examine the communication section of the plan for named primary and secondary mechanisms and confirm the secondary mechanism does not depend on the corporate email, identity or network. Examine exercise records for evidence that the backup channel was actually used, and confirm notification templates exist.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C17-09	EXAMINE	17.7: Examine the exercise programme, scenarios, attendance lists and exercise reports for the assessment period. Confirm at least one exercise in each twelve-month period involving key personnel, that it tested communication, decisions and workflow, and that actions were recorded and tracked to closure.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C17-10	OBSERVE	17.7: Where timing permits, observe a tabletop exercise and note whether participants follow the plan, use the notification matrix and can produce a draft CERT-In report within the six-hour window.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C17-11	SAMPLE	17.8: Select a sample of closed incidents meeting the review criteria and confirm a post-incident review was performed within the defined time, identified root cause and lessons learned, and produced actions with owners. Trace a sample of actions to evidence of completion.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C17-12	INSPECT	17.9: Inspect the incident classification and severity matrix for a definition distinguishing events from incidents and for categories such as abnormal activity, vulnerability, weakness, data breach and privacy incident. Confirm the categories map to CERT-In and DPDP reporting triggers. Sample SOC tickets and confirm the thresholds were applied consistently, and confirm annual review.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

Sampling Guidance

Base sampling on the assessment period, normally twelve months. Documentation Safeguards (17.1 to 17.6, 17.9) are tested by examining the current version and its review history, with contact verification sampled at around ten entries weighted to external authorities. For incident handling (17.4, 17.8), take the full population of reportable or high-severity incidents if fewer than ten, otherwise sample ten to fifteen, weighted to incidents involving personal data or regulatory re-

porting. For staff awareness of the reporting route (17.3), interview eight to twelve staff across functions, shifts and locations. For exercises (17.7), inspect every exercise in the period; the absence of any exercise in a twelve-month window is a failure of the annual requirement. Where the organisation had no real incidents, rely more heavily on exercises and on reconstructing whether SOC alerts that should have been declared incidents were in fact declared.

P Interview Questions

Interviewee	Question
Incident manager	If ransomware were found on a file server at 9 pm on a Saturday, what happens in the first six hours, and who files the CERT-In report?
DPO or privacy lead	How do you decide whether an incident is a personal data breach, and how would you prepare the intimations to the Data Protection Board and affected Data Principals?
Legal counsel	Which regulators, clients and insurers must be told of an incident, under which contracts or rules, and how quickly?
Employee (sample)	You have just clicked a link in a suspicious email. What do you do and whom do you tell?
MDR or IT provider	What does your contract require you to do when you detect an incident, and how quickly will you notify us?

Q Technical and Process Verification

- A named incident manager and deputy exist, understand their authority and have been reviewed within the year.
- The contact list and notification matrix are current, verified and available offline.
- Staff know how to report incidents, and reports reach the incident team promptly.
- The plan covers roles, regulatory obligations including CERT-In and DPDP, and communications, and has been approved and reviewed.
- Exercises are held at least annually and post-incident reviews lead to completed improvements.
- For IG3, thresholds and categories are defined, mapped to reporting triggers and applied consistently.

R Expected Evidence

- Incident response policy and plan with approvals
- Appointment records and RACI
- Verified contact list and notification matrix
- Staff reporting procedure and training material
- Incident register with detection and notification timestamps
- Copies of CERT-In, regulator and DPDP notifications made during the period
- Exercise reports and action trackers
- Post-incident review reports
- Incident classification and severity matrix

S Evaluation Criteria

Implemented

- All applicable Safeguards are documented, current and reviewed within the year, and staff and responders demonstrate awareness consistent with the plan.
- Sampled incidents were classified, escalated and notified within required windows, and reviews produced completed improvements.
- Exercises were held in each twelve-month period and tested communication, decisions and regulatory reporting.

Partially implemented

- A plan exists but omits regulatory notification duties, or has not been reviewed in over a year.
- Exercises or post-incident reviews occur but actions are not tracked to completion.
- The contact list exists but contains outdated or unverified entries, or has no offline copy.

Not implemented

- No one is designated to lead incident handling, or staff do not know how to report incidents.
- No documented incident response process exists for an IG2 enterprise.
- Reportable incidents occurred and were not reported to CERT-In or other required parties.

T Common Gaps and Findings

- Condition: the incident response plan lists CERT-In reporting but not DPDP breach intimation. Criteria: 17.4 requires compliance requirements in the plan; DPDP Act s.8(6) and Rules r.7 require intimation to the Board and Data Principals. Effect: a personal data breach may be reported late or not at all, exposing the organisation to penalties.
- Condition: the only incident communication channel is corporate email. Criteria: 17.6 expects primary and backup mechanisms. Effect: if the email tenant is compromised, the team cannot coordinate and the attacker may read the response.
- Condition: the contact list was last updated two years ago and the insurer's hotline number is wrong. Criteria: 17.2 expects annual verification. Effect: insurer notification may be late, risking cover under the policy.
- Condition: no exercise has been held since the plan was approved. Criteria: 17.7 expects at least annual exercises. Effect: the plan is untested and staff are unfamiliar with their roles.
- Condition: the MDR provider escalates alerts but the organisation has no internal owner for its work. Criteria: 17.1 requires internal oversight of providers. Effect: decisions on containment and notification are left to a third party or not taken.
- Condition: SOC analysts decide case by case what counts as an incident. Criteria: 17.9 expects defined thresholds. Effect: inconsistent escalation and missed reporting clocks.

U Remediation Guidance

- Add a regulatory notification section to the plan covering CERT-In, sector regulators and DPDP, with templates and named approvers.
- Set up an out-of-band secure messaging group and a conference bridge for the incident team, and test them in the next exercise.
- Verify every contact in the list within 30 days, keep an offline copy and set an annual reminder.
- Hold a tabletop exercise within the quarter using a ransomware-plus-data-theft scenario that tests both the six-hour and DPDP clocks.
- Appoint an internal owner for the MDR relationship and require them to approve containment and notification decisions.
- Publish an event and incident classification matrix mapped to reporting triggers and train SOC staff on it.

V Monitoring Metrics

- Percentage of reportable incidents notified to CERT-In within six hours of detection (target 100 per cent).
- Median time from first alert to incident declaration for high-severity incidents.
- Percentage of contact list entries verified in the last twelve months.
- Number of exercises held per year and percentage of exercise actions closed by due date.
- Percentage of significant incidents with a completed post-incident review within the defined time.

W Related Controls and Maturity Indicators

- Control 8 (audit logs provide evidence for investigation and meet CERT-In log requests)
- Control 11 (data recovery supports the recovery phase of response)
- Control 13 (monitoring generates the alerts that become incidents; 13.11 tuning uses lessons from 17.8)
- Control 14 (14.6 training staff to recognise and report incidents supports 17.3)
- Control 15 (service provider contracts define provider incident duties)
- Control 18 (penetration tests can exercise detection and response)

Initial	Defined	Managed	Optimised
Incidents are handled ad hoc by whoever notices them. There is no written plan and regulatory reporting depends on individual knowledge.	An incident manager, contact list, reporting procedure and plan exist and are approved, including regulatory notification duties, but have been little tested.	Roles, communication channels and thresholds are in use; exercises are held annually; incidents are reported within required windows and reviewed afterwards with tracked improvements.	Response performance is measured, exercises are frequent and varied, lessons feed detection and controls systematically, and the organisation coordinates smoothly with regulators, providers and peers.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A fictional Hyderabad hospital chain with six hospitals and 3,500 staff stores patient records in a hospital information system and uses a cloud email service. During a 2026 tabletop exercise run by its CISO, the scenario was a ransomware attack discovered at 11 pm that had encrypted the radiology archive and, according to the attacker's note, copied patient data.

The exercise exposed three problems. First, the incident manager's deputy had left the organisation months earlier and nobody had been named. Second, the team's only coordination channel was the corporate email system, which the scenario assumed was compromised. Third, the plan mentioned CERT-In but said nothing about the DPDP Act, so the team spent forty minutes debating whether patient notifications were needed and who would draft them.

Within a quarter the hospital named a new deputy, created an out-of-band messaging group and conference bridge, and added a notification matrix to the plan: CERT-In within six hours of noticing the incident, the Data Protection Board and affected patients under the DPDP Rules, and the cyber insurer within its policy terms. The DPO prepared templates for each, approved in advance by legal counsel. A severity matrix now marks any incident involving patient data as high severity, which starts the reporting clocks in the SOC ticket automatically.

When a real incident occurred later that year, a compromised clinician mailbox used to send phishing internally, the team declared an incident within 50 minutes of the first alert, filed the CERT-In report in under four hours and held a post-incident review that led to phishing-resistant MFA for clinical staff. The assessor rated 17.1 to 17.8 implemented and 17.9 implemented, noting a need to review thresholds after the first full year.

WP-C17: use the workpaper format shown in Appendix H.

CHAPTER 24 · CIS CONTROL 18

Penetration Testing

CIS CONTROL 18 · 5 SAFEGUARDS · 0 IN IG1

Penetration Testing

CIS Controls v8.1 · titles quoted verbatim | WP-C18

A Control Reference and Safeguards

CIS Critical Security Controls Version 8.1, Center for Internet Security, June 2024, Control 18 — Penetration Testing

Control 18 asks the organisation to find out whether its defences actually work by letting skilled people attack them under controlled conditions. Vulnerability scanning (Control 7) lists known weaknesses; penetration testing goes further by chaining weaknesses together, exploiting them, and showing what an attacker could really achieve, whether that is reading customer records, taking over the identity system or reaching an industrial controller. The Control has five Safeguards: a governing programme, annual external testing with reconnaissance, remediation of findings, validation of security measures after each test, and annual internal testing. None of them is in IG1, because penetration testing is only useful once the basic hygiene controls are in place; testing an unpatched, unmanaged estate mainly confirms what a scanner would already show. For IG2 and IG3 organisations, though, a well-run testing programme is one of the most direct sources of evidence that the other seventeen Controls are effective.

Control and Safeguard titles, asset types, security functions and Implementation Groups are from CIS Controls v8.1 (© CIS, CC BY-NC-ND 4.0). All explanation is in Srida IT's own words. For the authoritative Safeguard descriptions see cisecurity.org/controls.

Table 24-1. Safeguards of CIS Control 18, Penetration Testing

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
18.1	**“Establish and Maintain a Penetration Testing Program”**	Documentation	Govern	IG2	Penetration testing is run as a planned programme, not as one-off engagements. The programme fits the organisation's size, sector and maturity and writes down what is tested (networks, web applications, APIs, hosted and cloud services, physical premises), how often, the rules of engagement and exclusions, who the contacts are, how findings are routed and fixed, and how each test is reviewed afterwards.
18.2	**“Perform Periodic External Penetration Tests”**	Network	Detect	IG2	The internet-facing estate is tested from outside by a qualified tester at least once a year, and more often if the programme requires. Each test begins with reconnaissance of what an attacker could learn about the organisation and its environment, such as exposed services, leaked credentials, subdomains and staff information. The tester may work with full knowledge of the environment (clear box) or none (opaque box).
18.3	**“Remediate Penetration Test Findings”**	Network	Protect	IG2	Every finding from a penetration test is fixed, or formally accepted, through the organisation's documented vulnerability remediation process, with a timeline and effort set according to the finding's impact and priority.

Safeguard	Title (CIS wording)	Asset type	Function	From	What it means in practice (Srida IT)
18.4	**“Validate Security Measures”**	Network	Protect	IG3	After each test, the organisation checks whether its defences saw and stopped what the tester did, and where they did not, it changes detection rules, prevention settings or capabilities so that the same techniques would be caught next time.
18.5	**“Perform Periodic Internal Penetration Tests”**	Network	Detect	IG3	The internal network is tested at least yearly by a qualified tester simulating an attacker who has already got in, for example through a compromised laptop or a malicious insider, to see how far they can move and what they can reach. Clear-box or opaque-box approaches are both acceptable.

B Safeguard Implementation Guidance (Srida IT)

Safeguard	Practical steps	Evidence
18.1	**1.** Write a penetration testing standard that sets scope categories, minimum frequencies, tester qualification and independence requirements, rules of engagement (testing hours, prohibited techniques such as destructive denial-of-service, data handling) and emergency stop arrangements. **2.** Maintain a test calendar driven by risk, regulatory and contractual requirements and major changes, such as a new internet-facing application or a data-centre migration. **3.** Define how findings enter the vulnerability management process (Control 7), with owners and target dates, and require a retrospective after each test covering scope coverage, tester quality and what detection caught.	• Approved penetration testing standard or programme document • Test calendar for the current and previous year • Template rules of engagement and authorisation letter
18.2	**1.** Build the external scope from the asset inventory, DNS records, certificate transparency data and cloud accounts, and ask the tester to find anything the organisation missed. **2.** Select a qualified party, internal or external, with demonstrable skills and independence from the teams that built the systems; for regulated Indian entities, check whether a CERT-In empanelled auditor is required. **3.** Run the test under a signed authorisation and rules of engagement, including reconnaissance, exploitation within agreed limits and a report that separates confirmed exploits from scanner findings.	• External penetration test reports for each year in the period, with dates and scope • Signed authorisation and rules of engagement • Evidence of tester qualifications and independence
18.3	**1.** Log each finding in the vulnerability or risk tracking system with severity, owner and target date drawn from the remediation SLA in Control 7. **2.** Track progress and escalate overdue items; where a fix is not feasible, record a risk acceptance with compensating controls, approver and expiry date. **3.** Obtain retest evidence, from the original tester or an independent check, before closing high and critical findings.	• Finding tracker linked to each test report • Retest report or closure evidence for high and critical findings • Risk acceptances for findings not remediated

Safeguard	Practical steps	Evidence
18.4	**1.** Ask testers to provide a timeline of techniques used, with timestamps and source addresses, ideally mapped to a technique framework such as MITRE ATT&CK. **2.** Compare that timeline with SIEM, EDR, IDS/IPS and WAF records to identify which actions were detected, blocked, alerted but ignored, or missed. **3.** Raise changes to rules and capabilities for each gap and verify them, for example by replaying the technique in a later purple-team session.	• Detection gap analysis comparing tester activity with security tool records • Change records for rules or capabilities updated as a result • Retest or replay results confirming improved detection
18.5	**1.** Define the internal scope, including user networks, server and management zones, Active Directory or other identity stores, cloud workloads reachable from inside and, with great care, OT networks. **2.** Give the tester a realistic starting point such as a standard user laptop and account, and set objectives like reaching domain administrator rights, payment systems or the personal data store. **3.** Treat findings through the same remediation process as external tests, and use them to test segmentation (13.4) and detection (Control 13).	• Internal penetration test reports for each year, with scope and starting assumptions • Rules of engagement including OT or production safeguards • Remediation tracker entries for internal findings

C Implementation Group Expectations

IG1 · Essential cyber hygiene	IG2 · adds	IG3 · adds
Control 18 has no IG1 Safeguards. An IG1 organisation should concentrate on the hygiene Controls, especially vulnerability management (7.1 to 7.4) and secure configuration (Control 4). A small firm that is asked by a client for a test report may commission a limited external test of its website or customer portal, but this should not displace the IG1 basics.	IG2 has three Safeguards: a documented programme that sets scope, frequency, limits, contacts, remediation routing and retrospectives (18.1); external tests at least annually by a qualified party, including reconnaissance (18.2); and remediation of findings through the documented vulnerability process with impact-based timelines (18.3). Most mid-sized organisations meet IG2 with one well-scoped annual external test, application tests driven by Control 16 and a disciplined tracker.	IG3 adds two Safeguards: validating security measures after each test and adjusting detection and prevention where the tester went unnoticed (18.4), and annual internal penetration testing (18.5). Together they assume a mature monitoring capability under Control 13 and often lead to purple-team exercises or continuous adversary emulation in larger enterprises.

Implementation Groups are cumulative (IG2 includes IG1; IG3 includes IG1 and IG2). They express which Safeguards an enterprise should prioritise given its resources and risk; they are not maturity levels.

D ISO/IEC 27001:2022 Crosswalk

- 18.1 → 5.35 Independent review of information security; 8.8 Management of technical vulnerabilities; 8.34 Protection of information systems during audit testing
- 18.2 → 8.8 Management of technical vulnerabilities; 5.36 Compliance with policies, rules and standards for information security
- 18.3 → 8.8 Management of technical vulnerabilities; clause 10.2 Nonconformity and corrective action
- 18.4 → 8.16 Monitoring activities; 5.27 Learning from information security incidents; clause 10.1 Continual improvement
- 18.5 → 8.8 Management of technical vulnerabilities; 8.22 Segregation of networks; 8.34 Protection of information systems during audit testing

Indicative Srida IT mapping, not CIS's official mapping. Implementing a Safeguard does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST CSF 2.0 (Srida IT mapping): ID.RA-01 vulnerabilities identified (18.2, 18.5); ID.IM-02 improvements identified from security tests and exercises (18.4); ID.RA-06 risk responses chosen and tracked (18.3); GV.PO-01 policy (18.1)
- NIST SP 800-53 Rev. 5: CA-8 Penetration Testing; RA-5 Vulnerability Monitoring and Scanning; CA-2 Control Assessments; CA-5 Plan of Action and Milestones

- Related testing guidance: NIST SP 800-115, the OWASP Web Security Testing Guide and PTES are commonly used methodologies

F India Regulatory Touchpoints

- CERT-In empanelled information security auditing organisations: CERT-In maintains a list of empanelled auditors, and government entities and several regulators specify that audits and VAPT be conducted by them. CERT-In has also issued audit policy guidelines for organisations commissioning security audits
- SEBI CSCRF (2024): periodic VAPT of critical systems for regulated entities, with frequency by entity category, reporting of findings and closure timelines, and red teaming for the largest entities
- RBI cyber security and IT governance directions for banks and NBFCs: periodic VAPT of critical and internet-facing systems, with findings tracked to closure and reported to management
- DPDP Act 2023 s.8(5) and DPDP Rules 2025 r.6: periodic testing helps demonstrate that reasonable security safeguards for personal data are effective; any personal data encountered by testers must itself be protected

Mapping is not compliance. Confirm each obligation against the current instrument and your regulator's scope.

G Overview and Why It Matters

Controls that look sound on paper often fail in combination. A firewall rule added for a project, a forgotten test server, a service account with a weak password and a flat internal network may each be rated low risk, yet together they give an attacker a path from the internet to the database. Penetration testers find these paths because they think like attackers and are not bound by the assumptions of the teams who built the systems. External tests reveal what anyone on the internet can see and exploit; internal tests show what happens after the inevitable phishing success or insider misuse.

Testing without follow-through has little value. Organisations commonly receive a report, fix the easiest findings and file the rest, so the same issues reappear year after year. The Control therefore insists that findings are remediated through the normal vulnerability process and that each test is used to improve detection, so that the blue team learns from the red team rather than merely receiving a list of flaws.

In India, penetration testing is often driven by regulators and customers. SEBI's CSCRF, RBI directions and IRDAI guidelines expect periodic vulnerability assessment and penetration testing (VAPT) of critical systems, and government and many regulated-sector engagements specify testing by CERT-In empanelled information security auditing organisations. Enterprise customers of Indian SaaS and IT services firms routinely ask for recent third-party test reports in security questionnaires. A structured programme lets one test satisfy several of these needs, while the Control's emphasis on remediation and validation keeps the focus on reducing risk rather than collecting certificates.

I Applicability

The Control applies to IG2 and IG3 organisations generally, but scope varies a great deal. A small SaaS-first organisation with no servers of its own may have little external attack surface beyond its website and the SaaS tenant configuration; its external test can focus on the website, email security, identity provider settings and exposed cloud storage, while its SaaS providers' own test reports are reviewed under Control 15. Cloud-heavy organisations must check each provider's testing policy and notify or obtain permission where required before testing. OT environments need specialist testers and very conservative rules of engagement, often relying on passive analysis, testing of replica systems or maintenance windows, because active exploitation can halt production or cause safety incidents. Where IT is outsourced to an MSP, contracts should allow testing of the managed environment and require the MSP to remediate findings in its scope. In all cases the testing party must be independent of those who designed and operate the systems being tested, and testers' access to personal data must be minimised and protected.

J Implementation Guidance

1. Confirm readiness: the asset inventory, vulnerability scanning and patching (Controls 1, 2 and 7) are working, so that testing finds deeper issues rather than missing patches.
2. Write the penetration testing programme (18.1), covering scope categories, frequencies, tester qualification and independence, rules of engagement, contacts, remediation routing and retrospectives.
3. Plan the annual calendar, combining external tests, internal tests, application tests from 16.13 and any regulator- or customer-mandated tests so that one engagement serves several purposes.

4. Procure testers through a defined process that checks qualifications, references, insurance, data handling and, where required, CERT-In empanelment, and rotate providers or tester teams periodically to bring fresh perspectives.
5. Run the external test (18.2) with reconnaissance in scope, under a signed authorisation, with an emergency contact and stop procedure.
6. Run the internal test (18.5, IG3) from a realistic foothold with clear objectives, involving OT and production owners in the rules of engagement.
7. Load all findings into the vulnerability tracker (18.3), assign owners and dates by severity, retest critical and high findings, and record accepted risks with expiry dates.
8. Hold a validation session after each test (18.4, IG3) comparing tester activity with detection records, and raise rule and capability improvements.
9. Report programme results to management: findings by severity, overdue items, repeat findings and detection coverage improvements.

K Tools and Automation

- Vulnerability and finding tracker or GRC module: records each finding, owner, target date, retest status and risk acceptance.
- Attack surface discovery and reconnaissance tools: identify internet-facing assets, subdomains and exposed services before and between tests.
- Network and web testing tools used by testers, including open-source options such as Nmap, OpenVAS/Greenbone for initial discovery and OWASP ZAP for web applications.
- Breach and attack simulation or adversary emulation frameworks, including open-source ones, for repeatable validation of detections between full tests (18.4).
- SIEM and EDR consoles: provide the record of what defences saw during each test.
- Secure file exchange: protects test reports and any data extracted by testers.

Tool categories are indicative and vendor-neutral; Srida IT does not recommend specific commercial products.

L Roles and Responsibilities

Role	Responsibility
CISO or security lead	Owns the testing programme, approves scope and rules of engagement, and reports results to management
Penetration tester (internal or external)	Performs testing within the authorised scope and produces evidence-based reports and technique timelines
System and application owners	Agree test windows, provide access for clear-box testing and remediate findings
Vulnerability management lead	Tracks findings to closure, arranges retests and manages risk acceptances
SOC or detection engineer	Runs the post-test validation and updates detection rules
Procurement and legal	Contract testers with confidentiality, data handling, liability and authorisation terms

M Documentation and Records

- Penetration testing programme or standard
- Annual test calendar
- Rules of engagement and signed authorisation for each test
- Tester selection records, including qualifications, independence and any empanelment evidence
- Test reports and technique timelines
- Finding tracker, retest reports and risk acceptances
- Post-test validation and retrospective notes

N Assessment Testing Procedures

Recommended Srida IT assessment methodology. The CIS Controls define Safeguards; CIS does not prescribe these testing procedures.

Table 24-2. Assessment testing procedures, Control 18

Test ID	Method	Testing procedure	Result
TP-C18-01	**EXAMINE**	18.1: Examine the penetration testing programme document. Confirm it defines scope categories (network, web application, API, hosted or cloud services and, where relevant, physical controls), frequency, limitations and excluded techniques, points of contact, how findings are routed for remediation and the requirement for a retrospective. Confirm it has been approved and reviewed within the last year and reflects regulatory and contractual testing requirements.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C18-02	**INTERVIEW**	18.1: Interview the CISO or programme owner on how scope and frequency are decided, how testers are selected and how independence is ensured. Compare the answers with the test calendar and with procurement records for the testers used in the period.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C18-03	**EXAMINE**	18.2: Obtain the external penetration test reports for the assessment period and confirm at least one test in each twelve-month period. Examine each report for evidence of reconnaissance (asset discovery, exposed information, credential leakage), a defined clear-box or opaque-box approach and exploitation beyond automated scanning. Confirm the tested scope matches the internet-facing assets in the inventory and that any gaps are explained.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C18-04	**INSPECT**	18.2: Inspect the signed authorisation and rules of engagement for each external test, and the tester's qualification and independence evidence. Where the organisation is subject to regulatory requirements for a CERT-In empanelled auditor, confirm the tester appeared on the empanelled list at the time of testing.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C18-05	**SAMPLE**	18.3: Select a sample of findings from the test reports, including all critical and high findings and a sample of medium findings, and trace each into the vulnerability tracker. Confirm owner, target date consistent with the documented remediation SLA, closure or approved risk acceptance, and retest evidence for critical and high items. Identify any findings repeated from a previous year's report.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C18-06	**EXAMINE**	18.4: For each test in the period, examine the post-test validation record comparing tester activity with security tool logs. Confirm it identifies techniques detected, blocked and missed, that rule or capability changes were raised for missed techniques, and that a sample of those changes was implemented and verified.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C18-07	**RE-PERFORM**	18.4: Select one or two techniques that the validation record says are now detected and, with authorisation, re-run them in a controlled manner (or replay the relevant logs) to confirm an alert is generated and routed as expected.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C18-08	**EXAMINE**	18.5: Obtain the internal penetration test reports for the period and confirm at least one test in each twelve-month period. Examine the scope, starting assumptions and objectives, confirm that key internal zones and identity infrastructure were covered, and confirm that OT or sensitive production systems were either included under safe rules of engagement or excluded with a recorded reason.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A
TP-C18-09	**SAMPLE**	18.5: Sample internal test findings and trace them to remediation as in TP-C18-05, and confirm that findings relating to segmentation or lateral movement were shared with the network and SOC teams for action under Control 13.	☐ Impl. ☐ Partial ☐ Not impl. ☐ N/A

O Sampling Guidance

Testing is annual, so the population of test engagements is small and should be examined in full for the assessment period, normally the last twelve to twenty-four months so that two annual cycles can be seen. Within each test, examine every critical and high finding and a sample of around ten medium findings, choosing older and repeat items in preference. For validation (18.4), examine every post-test record and re-perform one or two techniques. Where the organisation relies on many application tests under 16.13, sample three to five application reports to confirm the programme governs them consistently. Compare the test scope with the current asset inventory rather than the inventory at the time of testing, so that unexplained growth in the attack surface is identified.

P Interview Questions

Interviewee	Question
CISO or programme owner	How did you decide the scope of last year's external and internal tests, and what was deliberately left out?
Vulnerability management lead	Which findings from the last test are still open, why, and who has accepted the risk?
SOC lead or detection engineer	During the last test, which tester actions did your tools detect, and what did you change afterwards?
Application or system owner	How were you involved in agreeing the test window and how did you remediate the findings in your system?
External tester (if available)	Did the rules of engagement or scope restrictions prevent you from testing anything you considered important?

Q Technical and Process Verification

- A documented programme governs all testing and has been reviewed within the year.
- External tests with reconnaissance were performed at least annually by qualified, independent testers.
- Findings were tracked, remediated within timelines or formally accepted, and critical and high items retested.
- For IG3, detection was validated after each test and gaps were closed.
- For IG3, internal tests were performed at least annually with realistic starting points and safe rules of engagement.

R Expected Evidence

- Penetration testing programme and test calendar
- External and internal test reports
- Authorisations and rules of engagement
- Tester qualification, independence and any CERT-In empanelment evidence
- Finding tracker with retest and closure evidence
- Risk acceptance records
- Post-test validation analyses and rule change records

S Evaluation Criteria

Implemented

- A current programme exists and annual external tests (and for IG3 internal tests) were performed by qualified, independent testers within the period.
- Critical and high findings were remediated and retested within timelines or formally accepted with compensating controls.
- For IG3, every test was followed by a validation exercise that led to verified detection improvements.

Partially implemented

- Tests are performed but without a governing programme, or more than twelve months elapsed between tests.
- Findings are tracked but many critical or high items are overdue without risk acceptance, or repeat findings recur.
- Validation after tests is informal and not evidenced.

Not implemented

- No external penetration test has been performed in the last twelve months.
- Test reports exist but findings are not tracked or remediated.
- For IG3, no internal penetration test has ever been performed.

T Common Gaps and Findings

- Condition: the most recent external test was 20 months ago. Criteria: 18.2 expects testing at least annually. Effect: new internet-facing services launched since then have never been tested.
- Condition: the external test report consists of automated scanner output with no exploitation or reconnaissance. Criteria: 18.2 expects reconnaissance and testing by a qualified party. Effect: chained or logic weaknesses remain undiscovered and the organisation has false assurance.
- Condition: seven high findings from last year's test are open and four appear again in this year's report. Criteria: 18.3 expects remediation through the documented process. Effect: known exploitable weaknesses remain available to attackers.
- Condition: testers obtained domain administrator rights without any SIEM alert, and no follow-up was performed. Criteria: 18.4 expects validation and rule changes after each test. Effect: a real attacker using the same path would go unnoticed.
- Condition: the same team that administers the firewall performs the annual external test. Criteria: 18.2 and the programme's independence requirement. Effect: tests reflect the team's own assumptions and conflicts of interest reduce credibility with regulators and customers.
- Condition: a regulated entity used a tester that was not on the CERT-In empanelled list where its regulator required one. Criteria: sector regulatory requirement. Effect: the test may not be accepted and a repeat engagement is needed.

U Remediation Guidance

- Commission an external test within the next quarter and adopt an annual calendar with tests scheduled before major releases.
- Specify in the tester contract that reconnaissance, manual exploitation and a technique timeline are required deliverables.
- Run a focused remediation sprint for overdue critical and high findings, record risk acceptances where fixes are not feasible, and add repeat findings as a management metric.
- Hold a validation workshop with the tester and SOC after every test and track resulting rule changes to verified closure.
- Separate the testing function from system administration, using an external tester or an independent internal team.
- Check regulatory and contractual tester requirements, including CERT-In empanelment, during procurement.

V Monitoring Metrics

- Number of months since the last external test and the last internal test (target 12 or fewer).
- Percentage of critical and high test findings closed within the remediation SLA.
- Number of findings repeated from the previous year's test.
- Percentage of tester techniques detected or blocked by security tools, trending upwards between tests.
- Percentage of internet-facing assets in the inventory covered by the last external test.

W Related Controls and Maturity Indicators

- Control 1 (the asset inventory defines test scope)
- Control 7 (vulnerability scanning and remediation processes receive test findings)
- Control 12 and 13.4 (segmentation is validated by internal tests)
- Control 13 (detection rules are validated and tuned after tests; 13.11)
- Control 15 (service provider testing evidence and contractual permission to test)
- Control 16 (16.13 application penetration testing)
- Control 17 (tests can exercise incident detection and response)

Initial	Defined	Managed	Optimised
Testing happens only when a customer or regulator asks, often as an automated scan, and findings are fixed opportunistically.	A testing programme with scope, frequency and rules of engagement exists, and annual external tests are performed by qualified testers.	External and internal tests are performed on schedule, findings are remediated within SLA and retested, and repeat findings are tracked as a metric.	Each test is followed by validation and purple-team work, detection coverage is measured against attacker techniques, and continuous testing or adversary emulation supplements the annual cycle.

Srida IT implementation-maturity indicators for this Control; distinct from Implementation Groups.

X Implementation Example and Workpaper

A fictional Bengaluru SaaS start-up with 180 employees sells an HR and payroll platform to Indian mid-market companies and hosts it on a public cloud. Several large customers, including a listed company subject to SEBI rules, asked for a recent third-party penetration test report, and one required that the tester be CERT-In empanelled.

Its first approach had been to share an annual automated scan. When a prospective customer's security team rejected that, the CTO and a newly hired security lead wrote a two-page testing programme: annual external and API testing by an independent firm, application testing of every major release under 16.13, an annual internal and cloud configuration test, and a 30-day retest window for high findings.

The external tester began with reconnaissance and found a forgotten staging subdomain exposing an older API version with weaker authorisation, a finding no scanner had flagged. They chained it with an insecure direct object reference to read another tenant's payslip data in the test environment. The start-up fixed both within ten days, decommissioned the staging host and added certificate transparency monitoring to its asset discovery.

After the test, the security lead compared the tester's timeline with the SIEM and cloud threat detection logs. Only three of eleven techniques had produced alerts. New rules for unusual API enumeration and cross-tenant access were added and later confirmed by replaying the tester's requests.

A year later the assessor found two annual external tests, one internal test, retests for every high finding and a documented validation record. 18.1 to 18.4 were rated implemented; 18.5 was partially implemented because the internal test had excluded the corporate identity provider without a recorded reason.

WP-C18: use the workpaper format shown in Appendix H.

PART III

Implementation

A practical programme: a 90-day IG1 roadmap, growing into IG2 and IG3, tooling and secure configuration baselines, one control set across CIS, ISO/IEC 27001, NIST CSF 2.0 and Indian regulation, and the Controls for SMEs, start-ups and managed service providers.

CHAPTER 25

IG1 Essential Cyber Hygiene: a 90-Day Roadmap

Implementation Group 1 is the floor, not a starter level that only small firms need. Every enterprise, whether it employs twelve people or twelve thousand, should be able to show that the 56 IG1 Safeguards are in place before it spends effort on anything more advanced. This chapter turns those 56 Safeguards into a practical 90-day plan that a small organisation can follow with its own staff, a part-time IT provider, or both. Larger enterprises can use the same sequence as a quick health check: if any IG1 item is missing, it goes to the top of the list, whatever else is planned.

The roadmap is a recommended order of work. It is Srida IT guidance, not part of the CIS Controls, and CIS does not prescribe a timetable. A firm that already has some of the pieces should skip ahead and spend the saved time on the items it lacks. A firm with almost nothing should accept that 90 days gives a working baseline, not a polished programme, and that the second quarter is for making the baseline routine.

25.1 Why a phased plan works for IG1

The IG1 Safeguards are not independent tasks. Several depend on each other, and doing them out of order wastes effort. You cannot patch, protect or back up devices you have not listed. You cannot review accounts without first knowing which systems hold them. Multi-factor authentication is far easier to switch on once you know which applications face the internet. The phases below follow these dependencies:

1. **Know what you have** (Days 1–20): devices, software, data, accounts and service providers.
2. **Shut the easy doors** (Days 21–45): passwords and MFA, administrator separation, default accounts, session locks, firewalls and the most urgent patching.
3. **Make protection automatic** (Days 46–65): automated patching, anti-malware, DNS filtering, supported browsers and email clients, encryption of end-user devices.
4. **Be ready to recover and respond** (Days 66–80): backups with an isolated copy, logging, incident contacts and a reporting route.
5. **Write it down and teach it** (Days 81–90): the documented processes, the awareness programme and the first review cycle.

Documentation sits at the end of the list as a phase, but in practice each process document should be drafted as the related work is done. Writing the secure configuration process while configuring the first laptop is quicker and more honest than writing it from memory three months later. Phase 5 is where those drafts are finished, approved and given a review date.

> **Govern Safeguards.**
>
> v8.1 tags a number of IG1 Safeguards with the Govern security function, mostly the "establish and maintain a process" items such as 3.1, 4.1, 4.2, 6.1, 6.2, 7.1, 7.2, 8.1, 11.1, 14.1, 17.2 and 17.3. For a small firm these can be short: one to three pages each, approved by the owner or managing partner, is usually enough. What matters to an assessor is that the document matches what people actually do and that someone reviews it at least once a year.

25.2 Before Day 1: appoint an owner and set the scope

Three decisions must be taken before the clock starts. First, name one person who owns the programme. In a 40-person firm this is often a partner or the office manager, supported by an outside IT provider; it should not be the provider alone, because the provider cannot accept risk on the firm's behalf. Second, define the scope: which offices, which cloud tenancies, which remote workers and which personal devices that touch firm data. Third, agree a weekly 30-minute check-in where the owner sees progress and decides on exceptions. These steps cost almost nothing and are the main reason small-firm programmes either finish or stall.

It also helps to decide early how progress will be recorded. A single spreadsheet with one row per IG1 Safeguard, a status column using the four-value scale from Chapter 6 (Implemented, Partially implemented, Not implemented, Not applicable), an evidence reference and a target date is sufficient. Appendix C provides an IG1 checklist that can serve as this tracker.

25.3 Phase 1 — Know what you have (Days 1–20)

The inventory phase covers Controls 1, 2, 3, 5 and 15. The goal is not perfection; it is a list good enough to act on, with an owner for each entry and a date for the next review.

- **Devices (1.1, 1.2).** Pull what you can from existing sources: the router or firewall's DHCP table, the cloud email tenant's device list, any MDM console, purchase invoices and a physical walk round the office. Record each device's name, owner, department, hardware address and whether it is approved. Agree what happens to an unknown device found on the network, and check for them every week.
- **Software (2.1, 2.2, 2.3).** List licensed software and SaaS subscriptions, with publisher, purpose and the date first used. Mark anything past its vendor's end of support. Unsupported software either goes or gets a written exception that names the compensating measures and the person accepting the risk. Repeat the support check monthly.
- **Data (3.2).** Identify where sensitive data lives: client files, payroll, Aadhaar and PAN copies, bank details, health records. A one-page register listing the data set, its location, its owner and who may access it is a sound start.
- **Accounts (5.1).** Export user lists from email, the accounting system, the file share and any line-of-business applications. Note user, administrator and service accounts separately, with start and leaving dates. Confirm each active account is authorised; this review should recur at least every quarter.
- **Service providers (15.1).** List the IT support firm, cloud hosts, payroll bureau, accounting software provider and anyone else who holds or reaches your data, with a named internal contact for each.

At the end of Phase 1 the owner should be able to answer five questions in a sentence each: how many devices, how many applications, where the sensitive data is, how many active accounts, and which outside parties hold data. If any answer is "we don't know", Phase 1 is not done.

25.4 Phase 2 — Shut the easy doors (Days 21–45)

Phase 2 deals with the weaknesses most often exploited in small-firm incidents: reused passwords, missing MFA, everyday use of administrator accounts and devices left with factory settings.

- **Unique passwords and MFA (5.2, 6.3, 6.4, 6.5).** Issue a password manager, set a minimum length, and turn on MFA for webmail, cloud storage, remote access and every administrator login. In most small firms this is a single tenant setting plus a week of helping staff enrol.
- **Dormant and administrator accounts (5.3, 5.4).** Disable accounts with no activity for 45 days where the system supports it, and remove leavers at once. Give each IT administrator a separate administrator account used only for administration.
- **Access granting and revoking (6.1, 6.2).** Agree a simple joiner–mover–leaver flow: who requests access, who approves it, and who removes it on the last working day.
- **Configuration basics (4.3, 4.4, 4.5, 4.6, 4.7).** Set screen locks to 15 minutes or less on computers and two minutes or less on mobiles, enable host firewalls on servers and laptops, change or disable default accounts on routers, printers and cameras, and manage devices over encrypted channels rather than plain HTTP or Telnet.
- **Network devices (12.1).** Check that the firewall, router and Wi-Fi access points run a supported, current firmware version, and set a monthly reminder to check again.

25.5 Phase 3 — Make protection automatic (Days 46–65)

Phase 3 replaces good intentions with settings that work without anyone remembering. The test of success is that a laptop left on a desk for a month comes back patched, scanned and encrypted.

- **Patching (7.3, 7.4).** Turn on automatic operating system updates and use the endpoint management tool or the application's own updater for browsers, office suites, PDF readers and other common applications. The cycle should be monthly at the latest.
- **Anti-malware (10.1, 10.2, 10.3).** Confirm every endpoint has active anti-malware with automatic signature updates, and switch off autorun for removable media.
- **Browsers, email and DNS (9.1, 9.2).** Remove unsupported browsers and email clients and point devices at a DNS filtering service that blocks known malicious domains.

- **Encryption (3.6).** Enable full-disk encryption on laptops and desktops and store recovery keys somewhere other than the device.
- **Data access (3.3, 3.4, 3.5).** Tighten file-share and cloud folder permissions to the people who need them, set retention periods for the main data sets, and agree how old disks and paper are destroyed.

25.6 Phase 4 — Be ready to recover and respond (Days 66–80)

- **Backups (11.2, 11.3, 11.4).** Back up in-scope systems automatically at least weekly, more often for critical data. Protect the backups with access restrictions and encryption, and keep one copy isolated from the main network or account, for example offline media or an immutable cloud copy with separate credentials. Ransomware that reaches the backup console is the most common reason small firms cannot recover.
- **Logging (8.2, 8.3).** Switch on audit logging in the email tenant, firewall, file server and key applications, and make sure there is enough storage to keep the logs. Indian organisations within the scope of the CERT-In Directions should note the expectation of log retention for a rolling 180 days within India, which is longer than many default settings.
- **Incident handling (17.1, 17.2, 17.3).** Name an incident lead and a deputy. Compile a contact sheet covering the IT provider, insurer, bank, legal adviser and, where relevant, CERT-In and sector regulators. Tell staff exactly how and to whom to report anything suspicious.

25.7 Phase 5 — Write it down and teach it (Days 81–90)

The final phase finishes the process documents (3.1, 4.1, 4.2, 6.1, 6.2, 7.1, 7.2, 8.1, 11.1, 17.3) and launches the awareness programme (14.1 to 14.8). Training for a small firm can be a one-hour session at induction plus short refreshers, covering phishing and social engineering, password and MFA habits, data handling, accidental exposure, reporting incidents, recognising devices that are missing updates, and the risks of public Wi-Fi. Keep attendance records; they are the evidence an assessor will ask for.

Day 90 closes with a review meeting. The owner walks through the tracker, confirms which Safeguards are Implemented, which are Partially implemented with a dated plan, and which are not applicable with a reason. That record becomes the baseline for the first self-assessment described in Chapter 30.

25.8 The roadmap at a glance

Table 25-1. 1 — The 56 IG1 Safeguards arranged into a 90-day plan (Srida IT sequencing)

Phase and days	Theme	IG1 Safeguards	Count	Typical evidence at the end of the phase
1 — Days 1–20	Know what you have	1.1, 1.2, 2.1, 2.2, 2.3, 3.2, 5.1, 15.1	8	Device, software, data, account and provider registers with owners and review dates
2 — Days 21–45	Shut the easy doors	4.3, 4.4, 4.5, 4.6, 4.7, 5.2, 5.3, 5.4, 6.1, 6.2, 6.3, 6.4, 6.5, 12.1	14	MFA enrolment report, admin account list, screen-lock and firewall settings, firmware versions
3 — Days 46–65	Make protection automatic	3.3, 3.4, 3.5, 3.6, 7.3, 7.4, 9.1, 9.2, 10.1, 10.2, 10.3	11	Patch compliance report, anti-malware console, DNS filter logs, encryption status, folder permission review
4 — Days 66–80	Recover and respond	8.2, 8.3, 11.2, 11.3, 11.4, 17.1, 17.2	7	Backup job history, isolated copy, log settings and storage, incident lead and contact sheet
5 — Days 81–90	Write it down and teach it	3.1, 4.1, 4.2, 7.1, 7.2, 8.1, 11.1, 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8, 17.3	16	Approved process documents, awareness content, attendance records, reporting procedure
Total			**56**	

Controls 13, 16 and 18 have no IG1 Safeguards, which is why they do not appear in the table. That does not mean an IG1 firm ignores network monitoring, application security or testing; it means CIS judges that the listed Safeguards give better

return first. Chapter 26 covers when to add them.

25.9 Week-by-week view for a small firm

Some owners prefer a weekly checklist. The table below spreads the same work across thirteen weeks for a firm with no full-time IT staff and roughly one day a week of outside support.

Table 25-2. 2 — Week-by-week IG1 schedule for a firm with part-time IT support

Week	Main activities	Owner sign-off question
1	Appoint owner, define scope, start device list (1.1)	Is every office, home worker and cloud tenant in scope?
2	Finish device list, set weekly unknown-device check (1.2), start software list (2.1)	Does every device have an owner?
3	Support status and exceptions (2.2, 2.3), data register (3.2), provider list (15.1), account list (5.1)	Which unsupported software remains and who accepted it?
4	Password manager, MFA for email and cloud (5.2, 6.3)	What percentage of staff are enrolled in MFA?
5	MFA for remote and admin access (6.4, 6.5), separate admin accounts (5.4), dormant accounts (5.3)	Does anyone still use an admin account for email?
6	Joiner–mover–leaver flow (6.1, 6.2), default accounts (4.7), screen locks (4.3)	Were last month's leavers removed on their last day?
7	Host firewalls (4.4, 4.5), secure management (4.6), network firmware (12.1)	Are any devices still managed over unencrypted channels?
8	Automated OS and application patching (7.3, 7.4)	How many devices are more than one month behind?
9	Anti-malware and autorun (10.1–10.3), browsers and DNS filtering (9.1, 9.2), disk encryption (3.6)	Are any endpoints unprotected or unencrypted?
10	Folder permissions, retention and disposal (3.3–3.5)	Who can open the payroll folder?
11	Backups with an isolated copy (11.2–11.4); logging and storage (8.2, 8.3)	Could we restore if the main account were taken over?
12	Incident lead, contacts and reporting route (17.1–17.3); finish process documents (3.1, 4.1, 4.2, 6.1, 6.2, 7.1, 7.2, 8.1, 11.1)	Does every staff member know where to report a suspicious email?
13	Awareness programme launch (14.1–14.8); Day-90 review	Which Safeguards are still only partially implemented, and by when will they be complete?

25.10 A worked example

A 40-person Kochi chartered accountancy firm (fictional) started the roadmap after a partner's mailbox was used to send fake invoice-change requests to two clients. It had cloud email, a single file server, around fifty devices including home laptops, and an IT vendor who visited on Saturdays.

In Phase 1 the firm found eleven devices nobody could account for, mostly old laptops still joined to Wi-Fi, and three former articled assistants whose accounts were still active. Phase 2 brought MFA to every mailbox within a fortnight; the main delay was helping two senior partners set up authenticator apps. Phase 3 revealed that automatic updates had been disabled on the file server years earlier to avoid reboots during filing season. The firm moved patching to a monthly Sunday window instead. Phase 4 was the turning point: the backup ran nightly to a USB drive that was always connected, so it would have been encrypted along with everything else in a ransomware attack. The firm added a weekly rotation of two drives, one kept at a partner's home, and a cloud copy under a separate administrator login.

At Day 90 the firm rated 49 Safeguards Implemented, five Partially implemented (mainly awareness training not yet delivered to all staff and two process documents still in draft) and two Not applicable with recorded reasons. It set a 30-day tar-

get for the partial items and scheduled its first formal self-assessment for the following quarter. The firm did not describe itself as having "achieved" IG1; it recorded the dated status and the plan, which is the accurate and defensible position.

25.11 India lens for the IG1 baseline

Several Indian obligations overlap with IG1 work, and the roadmap is a convenient time to address them. Mapping is not compliance; each obligation has its own scope and wording, which the firm must read.

- The **CERT-In Directions of 28 April 2022** expect covered entities to report specified incidents within six hours, synchronise clocks to designated time sources and retain logs for 180 days. The IG1 incident contacts (17.2) should include CERT-In's reporting route, and Phase 4 log settings should consider the retention period.
- The **DPDP Act 2023, section 8(5)**, requires a Data Fiduciary to take reasonable security safeguards to prevent personal data breaches, and the **DPDP Rules 2025** describe minimum safeguards and breach intimation in rules 6 and 7. The data register (3.2), access controls (3.3), encryption (3.6), backups (Control 11) and logging (Control 8) are practical building blocks for that duty.
- Regulated entities in banking, securities and insurance will find that IG1 falls well short of what RBI, SEBI or IRDAI expect, but it is still a useful check that the basics underneath the regulatory programme are sound.

25.12 Common pitfalls

- **Buying tools before listing assets.** A new endpoint product deployed to an incomplete inventory leaves gaps no one notices.
- **Writing policies nobody follows.** A downloaded 40-page policy is worse than a two-page process that matches practice. Assessors test against what the document says.
- **Treating the provider as the owner.** The IT vendor can do the work, but the firm must approve exceptions and accept risk.
- **Backups that share fate with production.** If the same credentials reach both, the backup is not isolated.
- **Stopping at Day 90.** Most IG1 Safeguards involve a recurring check: weekly unknown devices, monthly patching and support review, quarterly account review, annual document review. Put these in a calendar before the project team disbands.

25.13 After Day 90

The second quarter is for routine. Schedule the recurring checks, run the first self-assessment using Chapter 30's method, and decide whether the firm's environment, data and exposure justify moving towards IG2. Chapter 26 explains how to make that decision. For many small firms the honest answer is that IG1, done well and kept up, is the right target for the next year, with a handful of IG2 Safeguards added where a specific risk calls for them.

CHAPTER 26

Growing into IG2 and IG3

Implementation Groups describe the kind of enterprise a set of Safeguards is designed for, not a ladder that every organisation is expected to climb. IG2 adds 74 Safeguards for enterprises that run more varied infrastructure, hold more sensitive data, employ dedicated IT and security staff and face regulatory or contractual scrutiny. IG3 adds a further 23 for enterprises whose data or services would attract skilled, targeted attackers and whose failure would cause serious harm to the public or to other organisations. Cumulatively, IG2 is 130 Safeguards and IG3 is the full 153.

This chapter explains how to decide whether to move beyond IG1, how to sequence the IG2 work, where IG3 genuinely changes the picture, and how to avoid the trap of treating the Implementation Groups as a maturity score. Srida IT's maturity indicators (Initial, Defined, Managed, Optimised), used in each Control chapter, measure how well a Safeguard is run. The IG tells you which Safeguards are in scope. A firm can be at IG1 with Optimised operation of every Safeguard, or at IG3 with many Safeguards at Initial. The two scales answer different questions and should never be merged into one number.

26.1 Signals that it is time to look at IG2

CIS describes the IG profiles in general terms. In practice, Srida IT looks for the following signals when advising an enterprise whether to adopt IG2 as its target. Any two or three together usually justify the move.

Table 26-1. 1 — Signals that an enterprise should target IG2 or IG3 (Srida IT guidance)

Signal	Points towards IG2 when…	Points towards IG3 when…
Staffing	There is at least one person whose job is IT operations, or a managed provider on a full-service contract	There is a security team with specialist roles (monitoring, engineering, testing)
Data held	Personal data of customers or patients at volume, financial records, client confidential data	Data whose disclosure would cause significant public or national harm, or large-scale sensitive personal data
Regulation	Sector regulation applies (RBI, SEBI, IRDAI, health), or customers impose security clauses	The entity is designated critical, systemically important, or a market infrastructure institution
Technology	Several sites, cloud and on-premises mix, in-house or customised applications	Large estate, OT or safety systems, complex supply chain, internally developed products used by others
Exposure	Internet-facing services that customers depend on	Evidence of targeted attacks, or high-value target profile
Downtime tolerance	A day's outage causes real financial or reputational loss	Hours of outage cause safety, financial-stability or public-service harm

A 600-employee Pune NBFC (fictional) shows the logic. It holds customer KYC and loan data, is regulated by the RBI, runs a customer app and has an in-house IT team. It is clearly an IG2 enterprise. Whether it should go further depends on scale and on what its regulator expects; for most mid-sized NBFCs a well-run IG2 programme with selected IG3 Safeguards (for example, internal penetration testing and service provider monitoring) is a reasonable target.

26.2 What IG2 adds, Control by Control

IG2 is not evenly distributed. Some Controls gain one Safeguard; others are almost entirely IG2. The table below summarises the additions to help plan effort.

Table 26-2. 2 — New Safeguards added at IG2 and IG3, by Control (from canon)

Control	IG1	New at IG2	New at IG3	IG2 additions	IG3 additions
1	2	2	1	1.3, 1.4	1.5
2	3	3	1	2.4, 2.5, 2.6	2.7
3	6	6	2	3.7–3.12	3.13, 3.14

Control	IG1	New at IG2	New at IG3	IG2 additions	IG3 additions
4	7	4	1	4.8–4.11	4.12
5	4	2	0	5.5, 5.6	—
6	5	2	1	6.6, 6.7	6.8
7	4	3	0	7.5, 7.6, 7.7	—
8	3	8	1	8.4–8.11	8.12
9	2	4	1	9.3–9.6	9.7
10	3	4	0	10.4–10.7	—
11	4	1	0	11.5	—
12	1	6	1	12.2–12.7	12.8
13	0	6	5	13.1–13.6	13.7–13.11
14	8	1	0	14.9	—
15	1	3	3	15.2, 15.3, 15.4	15.5, 15.6, 15.7
16	0	11	3	16.1–16.11	16.12, 16.13, 16.14
17	3	5	1	17.4–17.8	17.9
18	0	3	2	18.1, 18.2, 18.3	18.4, 18.5
Total	**56**	**74**	**23**	Cumulative: IG2 = 130, IG3 = 153	

Three Controls dominate the IG2 workload: Control 16 (application software security, 11 new Safeguards), Control 8 (audit log management, 8 new) and Controls 3, 12 and 13 (six each). An enterprise that does not develop software can often mark much of Control 16 as Not applicable, but only with a documented reason; buying and configuring SaaS is not the same as developing software, yet customised low-code or scripted integrations frequently are. Chapter 30 covers how to record such scope decisions.

26.3 Sequencing the IG2 work

IG2 typically takes 12 to 24 months for a mid-sized enterprise starting from a sound IG1 base. Srida IT recommends four waves, each building on the last. The waves are guidance, not CIS requirements.

Wave A — Visibility (months 1–4)

The first wave makes the estate observable. Active discovery and DHCP log reconciliation (1.3, 1.4) and automated software inventory (2.4) keep the IG1 registers current without manual effort. Authenticated internal vulnerability scanning and monthly external scanning (7.5, 7.6) show where the gaps are, and a monthly remediation cycle driven by the IG1 remediation process (7.7) closes them. Centralised logging begins: synchronised time (8.4), richer log content (8.5) and collection of DNS, URL and command-line activity (8.6, 8.7, 8.8) into a central store (8.9) with at least 90 days' retention (8.10). For Indian entities under the CERT-In Directions, the 180-day expectation should drive the retention setting rather than the CIS minimum.

Wave B — Control of identity and network (months 4–9)

The second wave centralises who can do what and where. Service accounts get their own inventory and quarterly review (5.5). Account and access management move to a directory or identity provider (5.6, 6.7), with an inventory of the authentication systems themselves (6.6). The network gets a documented secure architecture and diagrams (12.2, 12.4), secure management protocols and centralised AAA (12.3, 12.5, 12.6) and a requirement that remote devices connect through a VPN tied to that AAA (12.7). Segmentation and filtering between segments (13.4) and access control for remote assets (13.5) follow naturally.

Wave C — Detection and hardening (months 9–15)

With visibility and identity in place, detection becomes meaningful. Security event alerting is centralised (13.1), host-based and network intrusion detection are deployed (13.2, 13.3) and flow logs are collected (13.6). Weekly log review (8.11) moves from manual reading to triage of alerts. Hardening extends to unnecessary services, trusted DNS, device lockout and remote wipe (4.8 to 4.11), browser and email extension control, DMARC and file-type blocking (9.3 to 9.6), and behaviour-based, centrally managed anti-malware with removable media scanning and anti-exploitation features (10.4 to 10.7). Application allowlisting (2.5, 2.6) belongs here too; it is the IG2 Safeguard that most often stalls, and it is better to start with servers and kiosks than with every laptop at once.

Wave D — Assurance and resilience (months 12–24)

The final wave proves that the programme works. Data recovery is tested quarterly on a sample (11.5). Data classification, data-flow documentation, removable-media and in-transit encryption, encryption at rest and segmentation by sensitivity (3.7 to 3.12) bring Control 3 up to the IG2 line. Service provider management gains a policy, classification and contractual security clauses (15.2 to 15.4). Incident response becomes a full process with roles, communication channels, exercises and post-incident reviews (17.4 to 17.8). Role-specific training (14.9) is delivered to administrators, developers and finance staff. A penetration testing programme with an annual external test and tracked remediation (18.1 to 18.3) closes the loop. Control 16 runs alongside Waves C and D for any enterprise that develops software.

> **Do not run the waves strictly in series.**
>
> Most enterprises have pressing items in later waves: a regulator's demand for a penetration test, or a customer contract requiring DMARC. Pull those forward. The waves show dependencies, not a mandatory order.

26.4 Where IG3 genuinely changes the picture

The 23 IG3 Safeguards fall into four groups. Recognising them helps an enterprise decide which IG3 items to adopt selectively even if it does not target IG3 in full.

- **Prevention instead of detection.** Host and network intrusion prevention (13.7, 13.8), port-level access control (13.9), application-layer filtering (13.10), script allowlisting (2.7), and data loss prevention (3.13). These assume the enterprise can tolerate and manage the operational risk of blocking.
- **Deeper visibility.** Passive asset discovery (1.5), logging of sensitive data access (3.14), collection of service provider logs (8.12) and monthly tuning of alert thresholds (13.11). These need analysts who will use the data.
- **Stronger governance.** Role-based access control with annual review (6.8), separate mobile workspaces (4.12), dedicated administrative workstations (12.8), service provider assessment, monitoring and secure decommissioning (15.5 to 15.7) and defined incident thresholds (17.9).
- **Adversarial assurance.** Code-level security checks (16.12), application penetration testing (16.13), threat modelling (16.14), validation of security measures against test findings (18.4) and internal penetration tests (18.5).

A Hyderabad hospital chain (fictional) with networked medical devices and a large patient database might adopt IG2 in full and then select 1.5 (passive discovery, because many medical devices cannot run agents and dislike active scans), 3.14 (logging access to patient records), 12.8 (dedicated admin workstations) and 15.5 to 15.7 (service provider assurance for its many clinical system vendors). That selective approach is legitimate, provided the enterprise records its target honestly: "IG2 plus named IG3 Safeguards", not "IG3".

26.5 Budgeting and resourcing

The cost of IG2 is driven more by people than by licences. Centralised logging without someone to review it produces a storage bill and no security. Before committing to IG2, an enterprise should confirm it has, or can contract for, the following capacities:

- an owner for log review and alert triage, at least weekly, ideally daily;
- an owner for vulnerability remediation who can negotiate patch windows with business teams;
- identity administration capacity to run the directory and quarterly account reviews;
- a network engineer, in-house or contracted, able to maintain segmentation and secure management;

- a person who manages service providers and their contracts;
- where software is developed, a security champion within the development team.

Managed services can supply several of these, as Chapter 29 discusses, but the enterprise must still own decisions about risk and exceptions.

26.6 Measuring progress without confusing IG and maturity

Report progress against the target IG as the percentage of in-scope Safeguards rated Implemented, with Partially implemented shown separately. Report maturity as a second dimension, for example the proportion of Safeguards at Managed or above. A board can then see both breadth (how many of the right things we do) and depth (how reliably we do them). Chapter 32 gives a reporting template.

Table 26-3. 3 — Two dimensions of progress that must be reported separately

Dimension	Question it answers	Scale	Example statement
Implementation Group coverage	Are we doing the Safeguards appropriate to our profile?	Implemented / Partially implemented / Not implemented / Not applicable, per Safeguard	"Of the 130 IG2 Safeguards, 118 are in scope; 92 are Implemented and 17 Partially implemented."
Srida IT maturity	How consistently and measurably do we run them?	Initial / Defined / Managed / Optimised, per Control	"Controls 5, 6 and 11 are Managed; Controls 8 and 13 remain Defined."

26.7 Common mistakes when moving up

- **Letting IG1 decay.** Teams busy with a SIEM project forget the monthly software support review. Re-test IG1 every year as part of the IG2 assessment.
- **Buying an IG3 product to compensate for an IG1 gap.** Data loss prevention does not help if the data inventory (3.2) is missing.
- **Declaring Not applicable to avoid work.** Every N/A needs a reason that would survive challenge, and should be revisited at each assessment.
- **Claiming an IG.** There is no CIS scheme that certifies an organisation at an Implementation Group. State the target and the measured status; do not present the IG as a badge.
- **Ignoring regulators.** IG2 and IG3 do not automatically satisfy RBI, SEBI CSCRF or IRDAI requirements. Use Chapter 28 to map the gaps.

26.8 A worked example: a Chennai auto-parts maker

A Chennai auto-parts manufacturer (fictional) with 1,200 employees, two plants with OT networks and a supplier portal had completed IG1 and wanted a three-year plan. Its assessment identified IG2 as the target with selected IG3 Safeguards for the plant networks.

Year one concentrated on Waves A and B for the corporate network: active discovery, central logging with 180-day retention to align with its reading of the CERT-In Directions, a directory-based identity platform and authenticated scanning. OT assets were inventoried using passive discovery (1.5, an IG3 Safeguard) because active scanning had previously caused a programmable controller to restart. Year two brought segmentation between IT and OT with filtering at the boundary (13.4), network intrusion detection on the OT span port (13.3) and dedicated administrative workstations for plant engineers (12.8). Year three focused on assurance: quarterly restore tests, supplier classification and contract clauses for its machine-tool vendors, and the first internal penetration test (18.5) scoped carefully to avoid production impact.

At each annual assessment the firm reported IG2 coverage and maturity separately, listed the IG3 Safeguards it had chosen and why, and recorded Not applicable items for Control 16 except the supplier portal, which it brought into scope. The board saw a steady rise in both dimensions without ever being told the firm was "IG3".

CHAPTER 27

Tooling, Automation and Secure Configuration Baselines

The CIS Controls are written to be technology-neutral, and so is this manual. No Safeguard requires a particular product, and none can be satisfied simply by buying one. Tools matter because many Safeguards recur on a weekly, monthly or quarterly cycle that people will not sustain by hand, and because evidence produced by a system is more reliable than evidence assembled for an audit. This chapter describes the tool categories that support the Controls, how to choose between them without favouring any vendor, how to automate the recurring work, and how to build and maintain secure configuration baselines, including the use of CIS Benchmarks as a reference.

27.1 Principles before products

Srida IT applies five principles when advising on security tooling for a CIS Controls programme.

1. **Inventory first.** Every tool that acts on assets depends on knowing which assets exist. A patching or anti-malware platform that covers 80 per cent of devices gives a misleading 100 per cent compliance figure for the 80 per cent it knows about.
2. **Use what you already own.** Modern operating systems, cloud tenants and network devices include capabilities that satisfy many Safeguards: built-in disk encryption, host firewalls, update services, audit logging, conditional access and DNS filtering. Switch these on and configure them before buying anything.
3. **One source of truth per data type.** Avoid three partial asset lists in three consoles. Decide which system is authoritative for devices, software, accounts and vulnerabilities, and feed the others from it.
4. **Evidence by design.** Prefer tools that keep history and can export reports. An assessor will ask for the state over a period, not just today.
5. **Fit the team.** A tool that needs a full-time engineer to run is the wrong choice for a firm with one IT generalist. Managed or cloud-delivered versions of the same category may be better.

27.2 Tool categories mapped to the Controls

The table below lists the main tool categories and the Controls they most directly support. It is not exhaustive, and most categories help several Controls. Open-source examples are named generically to show that capable non-commercial options exist; their suitability, licensing and support should be checked for each environment.

Table 27-1. 1 — Vendor-neutral tool categories and the Controls they support

Tool category	What it does	Primary Controls	Open-source examples (generic)
Configuration management database (CMDB) or asset register	Authoritative record of devices, software, owners and status	1, 2, 15	Several open-source asset management platforms exist
Active and passive discovery	Finds devices on the network by scanning or by listening to traffic	1	Nmap for active scanning; passive traffic analysers
Endpoint management and MDM	Deploys settings, software and updates to laptops and mobiles; reports inventory	1, 2, 4, 7, 10	osquery for inventory and state queries
Endpoint detection and response (EDR) and anti-malware	Detects and blocks malicious behaviour on hosts; records activity	10, 13	Wazuh (host-based detection), Velociraptor (investigation)
Patch management	Schedules and reports operating system and application updates	7	Operating system update services; package managers

Tool category	What it does	Primary Controls	Open-source examples (generic)
Vulnerability scanner	Authenticated and unauthenticated scanning of internal and external assets	7, 12, 16	OpenVAS/Greenbone
Identity provider and directory	Central accounts, MFA, single sign-on, access policy	5, 6, 12	Open-source directory and SSO servers
Privileged access management (PAM)	Controls and records use of administrator credentials	5, 6, 12	Open-source credential vaults and bastion hosts
Log collection and SIEM	Collects, stores, correlates and alerts on logs	8, 13, 17	Wazuh, open-source log pipelines and search stacks
Network intrusion detection or prevention	Inspects traffic for known attack patterns and anomalies	13	Suricata, Zeek
DNS and web filtering	Blocks known malicious or unwanted destinations; records queries	8, 9	Open-source DNS resolvers with blocklists
Email security and authentication	Filters malicious mail; enforces SPF, DKIM and DMARC	9	Open-source mail filters and DMARC report parsers
Backup and recovery	Automated, protected and isolated copies with tested restore	11	Open-source backup tools with encryption and deduplication
Data discovery and DLP	Finds sensitive data and controls its movement	3	Open-source pattern-matching scanners
Software composition analysis and code scanning	Identifies third-party components and code-level flaws	16	Open-source dependency checkers and static analysers
Governance, risk and compliance (GRC) register	Tracks Safeguard status, evidence, exceptions and actions	All, especially Govern Safeguards	Spreadsheets work at small scale

Naming an open-source tool here is not a recommendation for every environment. Commercial products in the same categories may suit some enterprises better. Whichever route is chosen, assess the tool's own security, support model and data location, and add it to the service provider inventory (15.1) if a third party operates it.

27.3 Choosing tools for different sizes of enterprise

The 40-person firm

A small firm on a cloud productivity suite can meet most of IG1 with the suite's own administration console, the operating system's built-in protections, a password manager, a DNS filtering service and a backup service that keeps an isolated copy. A spreadsheet can act as the asset, software, account and provider register. The key is to export reports regularly so that evidence exists for the quarter, not only for the day of the assessment.

The mid-sized enterprise

An organisation targeting IG2 usually needs a proper endpoint management platform, a vulnerability scanner with authenticated scanning, a central log platform, a directory-based identity provider with MFA and conditional access, and some form of network detection. Integration becomes the main concern: the scanner should read the asset register; the SIEM should know which devices are critical; tickets should flow from findings to the teams who fix them.

The large or highly exposed enterprise

IG3 environments add prevention-mode controls, DLP, PAM, application security tooling in the development pipeline and dedicated forensic capability. Here the risk is tool sprawl: dozens of consoles, overlapping agents and alerts nobody reads. An architecture review every year, asking which tools still earn their place, is part of good practice.

27.4 Automating the recurring Safeguards

Many Safeguards include a review cycle. Automation does not remove the need for human judgement, but it makes the cycle happen and leaves a record. The following table shows how common recurring checks can be automated.

Table 27-2. 2 — Automating recurring Safeguard activities

Safeguard	Recurring activity (paraphrased)	Automation approach	Evidence produced
1.2	Deal with unapproved devices every week	Discovery tool compares found devices with the register and raises a ticket for each unknown	Weekly unknown-device tickets with outcome
2.2	Check software support status every month	Inventory tool flags products past end of support; report sent to owner	Monthly support report, exception register
5.1, 5.5	Confirm all active accounts are authorised at least quarterly	Identity platform generates review campaigns to managers; non-responses escalate	Completed review campaign with decisions
5.3	Disable accounts inactive for 45 days	Scheduled script or identity policy disables accounts past the threshold	Job log, list of accounts disabled
7.3, 7.4	Patch operating systems and applications at least monthly	Patch platform with defined rings and deadlines	Monthly compliance report by device
7.5, 7.6	Scan internal assets quarterly and external assets monthly	Scheduled scanner jobs; results imported into ticketing	Scan history, ticket ageing
8.11	Review logs weekly for anomalies	SIEM correlation rules and dashboards; analyst sign-off on the weekly review	Review log with analyst initials and findings
11.2, 11.5	Back up at least weekly; test restores quarterly	Backup scheduler; scripted restore of a sample to an isolated environment	Job history, restore test reports
12.1	Check network device software versions monthly	Configuration management tool pulls versions and compares with vendor advisories	Monthly version report

> **Automation needs ownership.**
> A scheduled job that fails silently is worse than a manual task, because everyone assumes it ran. Every automated check should have a named owner who receives failure notices and confirms completion each cycle.

27.5 Secure configuration baselines

Control 4 asks for documented secure configuration processes for enterprise assets and software (4.1) and for network infrastructure (4.2). A baseline is the concrete outcome of that process: a written, versioned set of settings that every asset of a given type should have, with a record of approved deviations.

Sources for a baseline

Enterprises rarely need to write baselines from nothing. Common starting points include:

- **CIS Benchmarks**, consensus-developed configuration guides for many operating systems, cloud platforms, databases, network devices and applications. They typically offer more than one profile level, so that an enterprise can choose a set that balances security and operational impact. CIS also publishes hardened images and configuration assessment tooling; check current availability, licensing terms and which items are free for non-commercial use before relying on them.
- **Vendor security guides** published by operating system, cloud and network equipment makers.
- **Government guidance**, including advisories and hardening guides issued by CERT-In and other national agencies.
- **Regulatory expectations**, where a sector regulator prescribes specific settings or controls.

Using a CIS Benchmark as a source does not make the enterprise "CIS compliant", and the Benchmark does not replace the enterprise's own documented process under 4.1. The enterprise must still decide which recommendations to adopt, record why others are excluded, and test that the result works in its environment.

Building the baseline

1. **Define asset types.** Group assets that share a configuration: Windows laptops, Linux web servers, firewalls, mobile phones, cloud storage accounts.
2. **Select a reference.** Choose a benchmark or vendor guide per type and a profile level.
3. **Tailor.** Walk through each recommendation with the system owner. Mark each as adopted, adopted with modification, or excluded with a reason.
4. **Test.** Apply the baseline to a pilot group and monitor for breakage. Expect a few iterations.
5. **Encode.** Express the baseline in the management tool: group policy, MDM profiles, configuration scripts, infrastructure-as-code templates or golden images.
6. **Measure.** Use a configuration assessment tool to compare actual settings with the baseline and report drift.
7. **Maintain.** Review the baseline at least annually and when the reference publishes a new version or the platform changes.

Minimum content of an IG1 baseline

For a small enterprise, a short baseline per asset type that covers the IG1 configuration Safeguards is enough. It should state at least the session lock period (4.3), host firewall settings (4.4, 4.5), how the device is managed securely (4.6), what happens to default accounts (4.7), disk encryption (3.6), automatic updates (7.3, 7.4), anti-malware and autorun (10.1 to 10.3), DNS filtering (9.2) and which browsers and email clients are permitted (9.1).

Table 27-3. 3 — Example IG1 baseline outline for company laptops

Setting area	Baseline value (example)	Safeguard	How enforced
Screen lock	Lock after 10 minutes of inactivity; password or biometric to unlock	4.3	MDM or group policy
Host firewall	On for all profiles; inbound denied except approved management	4.5	MDM or group policy
Local admin	Default administrator disabled or renamed with unique password; users not local admins	4.7, 5.4	Endpoint management
Disk encryption	Full-disk encryption on; recovery key escrowed centrally	3.6	MDM
Updates	Automatic OS and application updates; deadline 14 days after release	7.3, 7.4	Patch platform
Anti-malware	Real-time protection on; automatic signature updates; autorun disabled	10.1–10.3	Endpoint protection console
DNS	Enterprise DNS filtering resolver enforced	9.2	Network settings or agent
Browsers and email	Only approved, supported versions installed	9.1	Software inventory and removal

The values in this table are illustrations. Each enterprise sets its own, within the limits set by the Safeguards; for example, the general-purpose session lock must not exceed 15 minutes.

Network infrastructure baselines

Network devices deserve a separate baseline under 4.2 because they are managed differently and often by different people or providers. Typical content covers supported firmware (12.1), disabling unused services and interfaces, removing or changing default credentials, management only over encrypted protocols, logging to a central collector with synchronised time, configuration backups and change control. For outsourced networks, the baseline should be referenced in the provider's contract and its status reported regularly.

Cloud and SaaS baselines

Cloud tenancies drift quickly because settings can be changed through consoles, APIs and automation by many people. A cloud baseline should cover identity (MFA, conditional access, privileged role assignments), logging (tenant audit logs on, retained and exported), storage (public access blocked by default, encryption on), network exposure and key management. Cloud security posture management tools, and the native policy engines of the major platforms, can continuously compare settings with the baseline.

27.6 Managing exceptions

Some assets cannot meet the baseline: a laboratory instrument running an old operating system, a legacy finance application that needs a deprecated protocol, an OT controller that cannot run an agent. Each exception should be recorded with the asset, the deviation, the reason, compensating measures, an owner who accepts the risk and an expiry date. An exception without an expiry date tends to become permanent. Assessors will sample exceptions and check that they are still valid.

27.7 India lens on tooling

- Where log or security data is stored by a cloud tool, check whether any Indian obligation requires it to be kept in India. The CERT-In Directions refer to logs being maintained within Indian jurisdiction, and some sector regulators set data localisation expectations.
- Clock synchronisation (8.4) should use time sources acceptable under the CERT-In Directions, which refer to NIC and NPL servers or traceable equivalents.
- Tools that process personal data, such as DLP, email security or SIEM, are themselves processing activities under the DPDP Act 2023 and should be covered by the enterprise's privacy notices and processor contracts where relevant.

27.8 A worked example: a Bengaluru SaaS start-up

A 90-person Bengaluru SaaS start-up (fictional) had no on-premises servers. Every engineer used a company laptop, production ran in one public cloud account and the office network was a single managed Wi-Fi. The founders wanted IG1 quickly and IG2 within 18 months to satisfy enterprise customers.

For IG1 the start-up used its productivity suite's device management to enforce disk encryption, screen lock, firewall and updates, and exported weekly device compliance reports to a shared drive. It adopted CIS Benchmark guidance for its laptop operating system and cloud account as reference points, tailoring a small number of settings that broke developer tooling and recording each exclusion. For IG2 it added a cloud posture tool that compared the account with its tailored baseline every hour, an open-source host intrusion detection agent on build servers, centralised logging into a managed search platform with 180-day retention, and dependency scanning in its build pipeline for Control 16.

The most valuable step was not a tool at all. The start-up agreed that every production change would go through infrastructure-as-code reviewed by a second engineer, which made configuration drift visible and turned the baseline from a document into the way the platform was built.

CHAPTER 28

One Control Set: CIS with ISO/IEC 27001, NIST CSF 2.0 and Indian Regulation

Few Indian enterprises use the CIS Controls in isolation. A software exporter may hold ISO/IEC 27001 certification for its customers, a listed company may report against NIST CSF 2.0 language to its board, and a regulated entity must satisfy CERT-In, its sector regulator and the DPDP Act. Running separate programmes for each produces duplicate evidence, inconsistent answers and audit fatigue. This chapter shows how to use the CIS Safeguards as the operational layer of a single control set, with ISO/IEC 27001 as the management system, NIST CSF 2.0 as the outcome language, and Indian obligations as additional requirements mapped onto the same controls.

> **Status of the mappings.**
>
> The crosswalks in this chapter are Srida IT mappings prepared for practical use. They are not official CIS, ISO or NIST mappings. CIS publishes its own mappings to several frameworks on its website, and those should be consulted for authoritative alignment. A mapping shows where two frameworks address related topics; it does not mean that meeting one satisfies the other. Mapping is not compliance.

28.1 Why the CIS Controls make a good operational layer

Each framework has a different shape. ISO/IEC 27001:2022 specifies a management system (clauses 4 to 10) and offers 93 reference controls in Annex A, which an organisation selects through risk assessment and records in its Statement of Applicability. NIST CSF 2.0 describes outcomes across six functions, Govern, Identify, Protect, Detect, Respond and Recover, without prescribing how to reach them. Indian regulations set obligations, often with time limits and reporting duties, but usually leave the technical means to the regulated entity.

The CIS Safeguards are specific, prioritised and testable. They say what to do, with a stated frequency where relevant, and they are grouped by enterprise profile. That makes them a natural answer to the question every other framework leaves open: “what, concretely, should our technical teams be doing?” The resulting structure has three layers:

1. **Governance and management system:** ISO/IEC 27001 clauses 4 to 10, and the CSF 2.0 Govern function. Context, leadership, risk assessment, objectives, competence, internal audit, management review and improvement.
2. **Control catalogue:** the CIS Safeguards for the chosen Implementation Group, supplemented by any ISO Annex A controls or regulatory requirements that CIS does not cover, such as physical security or human-resources screening.
3. **Obligation register:** each Indian legal or regulatory requirement, linked to the Safeguards and other controls that address it, with the evidence an inspector would expect.

28.2 CIS Controls and ISO/IEC 27001:2022

The CIS Controls do not replace an ISMS. They provide no equivalent of clauses 4 to 10, which cover the organisation's context, leadership commitment, risk assessment and treatment, support, operation, performance evaluation and improvement. An enterprise seeking ISO/IEC 27001 certification still needs those clauses. What the CIS Controls supply is a well-structured, testable set of technical and operational controls that can be referenced from the Statement of Applicability and that explain how many Annex A controls are implemented.

Equally, Annex A contains topics the CIS Controls touch only lightly or not at all: physical and environmental security (section 7), much of people security (section 6), threat intelligence (5.7), information security in project management (5.8), intellectual property (5.32) and business continuity (5.29, 5.30). An integrated control set must add these.

Table 28-1. 1 — CIS Controls v8.1 to ISO/IEC 27001:2022 Annex A, summary crosswalk (Srida IT mapping)

CIS Control	Principal Annex A controls	Notes
1 Enterprise assets	5.9, 8.1	Annex A 5.9 covers information and other assets more broadly

CIS Control	Principal Annex A controls	Notes
2 Software assets	5.9, 8.19	Allowlisting supports 8.19 installation of software on operational systems
3 Data protection	5.12, 5.13, 5.14, 5.33, 5.34, 7.10, 7.14, 8.10, 8.11, 8.12, 8.24	Privacy obligations (5.34) extend beyond CIS scope
4 Secure configuration	8.1, 8.9, 8.20	8.9 configuration management is the closest single match
5 Account management	5.16, 5.17, 5.18, 8.2	
6 Access control	5.15, 5.18, 8.2, 8.3, 8.5	MFA Safeguards align with 8.5 secure authentication
7 Vulnerability management	8.8, 8.19	
8 Audit logs	8.15, 8.16, 8.17	Clock synchronisation (8.4 in CIS) aligns with Annex A 8.17
9 Email and browser	8.7, 8.23	DMARC has no direct Annex A equivalent
10 Malware defences	8.7	
11 Data recovery	8.13, 5.30	5.30 ICT readiness is broader than backup
12 Network infrastructure	8.20, 8.21, 8.22	
13 Network monitoring	8.16, 8.20, 8.22, 8.23	
14 Awareness and training	6.3, 6.8	Clause 7.2 competence and 7.3 awareness also apply
15 Service providers	5.19, 5.20, 5.21, 5.22, 5.23	
16 Application security	8.25, 8.26, 8.27, 8.28, 8.29, 8.31	
17 Incident response	5.24, 5.25, 5.26, 5.27, 5.28, 6.8	
18 Penetration testing	8.8, 8.29, 5.35	5.35 independent review is broader than testing

Appendix F extends this summary to the Safeguard level. Where an Annex A control maps to several CIS Safeguards, the Statement of Applicability can cite the Safeguards as the implementation, and the CIS assessment results become evidence for ISO internal audit (clause 9.2).

Using CIS within the ISO risk process

ISO/IEC 27001 requires controls to be selected through risk assessment and treatment (clauses 6.1.2 and 6.1.3). The CIS Implementation Groups offer a defensible starting point: the IG1 Safeguards are a baseline nearly every risk assessment will justify, and IG2 or IG3 Safeguards can be selected where risks warrant them. The Statement of Applicability should still record why each control is included or excluded. Saying "because CIS IG2 includes it" is weaker than linking the control to identified risks; the strongest position does both.

28.3 CIS Controls and NIST CSF 2.0

CIS v8.1 assigns each Safeguard a security function. With v8.1, CIS added Govern to the five functions already used, bringing its labels into line with the six functions of CSF 2.0. This makes the two frameworks easy to align at the function level. At the Subcategory level the mapping needs care, because CSF outcomes are broader and one Subcategory often relates to several Safeguards.

Table 28-2. 2 — Selected CIS Safeguards and related NIST CSF 2.0 Subcategories (Srida IT mapping)

CIS Safeguards	CSF 2.0 Subcategory	Relationship

CIS Safeguards	CSF 2.0 Subcategory	Relationship
1.1, 1.3, 1.4, 1.5	ID.AM-01 (hardware inventories)	Safeguards describe how the inventory is built and kept current
2.1, 2.4	ID.AM-02 (software, services and systems inventories)	Direct
3.2	ID.AM-07 (data inventories)	Direct
3.8	ID.AM-03 (network communication and data flows)	Partial
15.1	ID.AM-04 (supplier services inventories) and GV.SC-04	Partial
5.1–5.6, 6.1, 6.2	PR.AA-01 (identities and credentials managed)	Direct
6.3–6.5	PR.AA-03 (users, services and hardware authenticated)	Direct
6.8	PR.AA-05 (access permissions and authorisations managed)	Direct
3.6, 3.11	PR.DS-01 (data at rest protected)	Direct
3.10	PR.DS-02 (data in transit protected)	Direct
11.2–11.5	PR.DS-11 (backups created, protected, maintained and tested)	Direct
4.1–4.12	PR.PS-01 (configuration management practices)	Direct
7.3, 7.4, 2.2	PR.PS-02 (software maintained, replaced and removed)	Direct
8.2, 8.5–8.8	PR.PS-04 (log records generated)	Direct
2.5–2.7	PR.PS-05 (unauthorised software prevented)	Direct
16.1–16.14	PR.PS-06 (secure software development)	Direct
7.1, 7.5, 7.6	ID.RA-01 (vulnerabilities identified)	Direct
13.1–13.3, 13.6	DE.CM-01 (networks monitored) and DE.CM-09 (computing environments monitored)	Partial
14.1–14.9	PR.AT-01 and PR.AT-02 (awareness and role-based training)	Direct
15.4	GV.SC-05 (requirements in supplier contracts)	Direct
17.2, 17.3, 17.6	RS.CO-02 (stakeholders notified of incidents)	Partial

CSF 2.0's Govern function is wider than the CIS Govern-tagged Safeguards. It includes organisational context, risk management strategy, roles and authorities, policy, oversight and supply chain risk management. An enterprise reporting in CSF language should use the CIS Govern Safeguards as evidence for parts of GV.PO (policy) and GV.SC (supply chain), and supply the remainder from its ISMS or governance framework.

Srida IT's sister manual on NIST CSF 2.0 provides Subcategory-level testing procedures that can be combined with this manual's Safeguard tests where an enterprise reports in both frameworks.

28.4 Indian regulation

Indian cyber security and data protection obligations are spread across several instruments. Each has its own scope, definitions and timelines, and each should be read in full by the enterprise and its advisers. The summary below identifies where the CIS Controls provide useful technical support. All specifics are marked for verification because regulatory texts and circulars change frequently.

Table 28-3. 3 — Indian obligations and the CIS Controls that support them (Srida IT mapping; mapping is not compliance)

Instrument	Who it applies to	Examples of what it expects	Supporting CIS Controls

Instrument	Who it applies to	Examples of what it expects	Supporting CIS Controls
CERT-In Directions under section 70B(6) of the IT Act, 28 April 2022	Service providers, intermediaries, data centres, body corporates and government organisations, with specific categories for some duties	Report specified incidents within six hours; synchronise clocks to designated sources; retain logs for 180 days in India; designate a point of contact	8 (logging, time, retention), 17 (reporting and contacts)
SEBI Cybersecurity and Cyber Resilience Framework (CSCRF), 2024	SEBI-regulated entities, graded by category	Governance, asset identification, protection, detection, response and recovery, audits and reporting proportionate to category	Broadly all 18; especially 1–3, 5–8, 11, 13, 17, 18
RBI directions on IT governance, risk, controls and assurance, and cyber security frameworks	Banks, NBFCs and other RBI-regulated entities as specified	Board-level IT and cyber governance, risk management, security operations, vulnerability assessment and penetration testing, incident reporting to the RBI	Broadly all 18; Govern Safeguards support board reporting
IRDAI information and cyber security guidelines	Insurers and insurance intermediaries	Information security governance, policies, audits, incident reporting	Broadly all 18
DPDP Act 2023, section 8(5), and DPDP Rules 2025, rules 6 and 7	Data Fiduciaries processing digital personal data	Reasonable security safeguards including encryption, access control, logging and monitoring, backups; breach intimation to the Data Protection Board and affected Data Principals	3, 5, 6, 8, 11, 15, 17
CERT-In empanelled audits	Entities required by a regulator or contract to use an empanelled auditor	Independent security audit by an auditing organisation on CERT-In's empanelled list	Assessment results under Part IV provide input; they do not replace the audit

Building the obligation register

For each instrument that applies, list the individual requirements as separate rows. For each row, record the source reference, the requirement in the enterprise's own words, the owner, the controls that address it (CIS Safeguards, Annex A controls or other), the evidence, and any gap. For example, a row for the CERT-In six-hour reporting requirement would link to 17.1 (incident handling personnel), 17.2 (contact information, including CERT-In), 17.3 (reporting process) and, at IG2, 17.4 and 17.6. Its evidence would include the incident procedure showing the six-hour clock, the contact sheet, and the record of the last exercise or real report.

Where an Indian requirement is stricter than the CIS Safeguard, the stricter requirement governs. Log retention is the obvious case: CIS 8.10 sets a 90-day minimum, while the CERT-In Directions expect 180 days, and some sector regulators or the DPDP Rules may expect longer for particular logs. Record the higher figure in the audit log management process (8.1).

28.5 Running one assessment for several frameworks

Once the control set is unified, one testing cycle can produce evidence for several purposes. Srida IT recommends the following approach.

1. **Test once, at the Safeguard level,** using the procedures in Part II. Record the result on the four-value scale.
2. **Roll up by mapping** to Annex A controls, CSF Subcategories and regulatory rows. Where several Safeguards map to one item, the item is only as strong as its weakest relevant Safeguard, unless the enterprise records a reasoned judgement otherwise.
3. **Add the non-CIS tests** for topics outside CIS scope, such as physical security or HR screening.
4. **Report in the audience's language:** Annex A for the certification body, CSF functions for the board, the regulator's own structure for regulatory returns.

This approach reduces duplicated sampling. It does not remove the need for an ISO certification audit by an accredited body, a regulator-mandated audit, or a CERT-In empanelled audit where these are required. Internal assessments using

this manual are preparation for, and inputs to, those processes.

28.6 A worked example

A 600-employee Pune NBFC (fictional) held ISO/IEC 27001 certification for its data centre, reported to its board using CSF 2.0 functions and was subject to RBI directions, the CERT-In Directions and the DPDP Act. Its security team had three separate trackers and was answering the same evidence request three times a year.

It rebuilt its control set around the 130 IG2 Safeguards plus selected IG3 items, added 22 Annex A controls that CIS did not cover, and created an obligation register of 64 rows drawn from the RBI directions, CERT-In Directions and DPDP Rules. Each Safeguard test produced one workpaper; the GRC tool rolled results up to Annex A for the surveillance audit, to CSF functions for the board pack, and to the regulatory rows for the compliance function. The first integrated cycle exposed two real gaps that the separate trackers had hidden: log retention for the loan origination system was 90 days, not the 180 days the team believed, and the incident procedure had no step to notify the Data Protection Board. Both were fixed before the next regulatory inspection.

CHAPTER 29

The CIS Controls for SMEs, Start-ups and Managed Service Providers

Most organisations in India are small. Micro, small and medium enterprises form the overwhelming majority of registered businesses, and many of them handle client data, payments or personal information on behalf of larger firms. They are also frequent targets: attackers use them as soft entry points into the supply chains of banks, manufacturers and government departments, or simply as easy sources of fraud and ransom. Yet most security frameworks are written with a large enterprise in mind. The CIS Controls are unusual in that the first Implementation Group is explicitly designed to be achievable by an organisation with limited IT and security expertise. This chapter explains how SMEs, start-ups and the managed service providers (MSPs) who support them can apply the Controls realistically.

29.1 SMEs: doing IG1 with what you have

The resource reality

A typical Indian SME of 20 to 200 people might have one office manager who looks after IT, a local vendor who visits when something breaks, a cloud email subscription, an accounting package, a few shared folders and a mixture of company and personal phones. Budgets for security are small and compete with growth spending. Any approach that requires a dedicated security officer or a SIEM will not happen.

The good news is that IG1 does not require those things. Of the 56 IG1 Safeguards, the large majority can be met with built-in features of the operating systems and cloud services the firm already pays for, a password manager, a DNS filtering service, a backup service with an isolated copy, a handful of short written processes and an hour of staff training. Chapter 25 sets out a 90-day plan; the points below adapt it to the constraints SMEs most often face.

Practical adaptations

- **Registers in one workbook.** Keep the device, software, data, account and service provider inventories (1.1, 2.1, 3.2, 5.1, 15.1) as tabs in a single spreadsheet with an owner and review date on each tab. Store it in a location with version history.
- **Personal devices.** Where staff use their own phones for email, enrol them in the cloud suite's lightweight app management so that firm data can be protected and wiped without managing the whole phone. Record which personal devices are in scope; they count for 1.1.
- **Shared logins.** Shared accounts for the accounting package or a supplier portal are common in small firms and directly conflict with unique passwords (5.2) and access control. Most providers now support named users at low cost; switch to them and close the shared login.
- **The owner as administrator.** Founders often hold the only global administrator role and use it for everyday email. Create a separate administrator account (5.4), protect it with strong MFA (6.5), and keep a sealed break-glass credential.
- **Backups that actually restore.** A USB drive permanently plugged into the file server is not an isolated copy (11.4). Rotate drives or use a cloud backup with separate credentials and immutability.
- **Short documents.** A two-page process that matches practice is better than a template that does not. The Govern Safeguards need content, not length.

What an SME can reasonably defer

An IG1 SME does not need network intrusion detection, a SIEM, application allowlisting, formal penetration testing or a secure development lifecycle unless a specific risk or customer requirement calls for them. It should, however, keep an eye on a small number of IG2 Safeguards that are cheap and high-value even for small firms: DMARC (9.5) to reduce email spoofing of the firm's domain, testing a restore every quarter (11.5), and a service provider policy and contract clauses (15.2, 15.4) for the IT vendor who holds administrator access.

Table 29-1. 1 — Low-cost IG2 Safeguards worth considering early in a small firm (Srida IT guidance)

Safeguard	Why it is worth doing early	Typical effort for a 40-person firm
9.5	Invoice and payment-change fraud often spoofs the firm's own domain	A few DNS records and a monitoring period before enforcing
11.5	Untested backups regularly fail when needed	One hour per quarter to restore a sample folder and mailbox
15.4	The IT vendor usually holds the keys to everything	A one-page security schedule added to the vendor's contract
5.6 / 6.7	Single sign-on through the cloud suite reduces password sprawl	Configuration of SSO for the main SaaS applications
4.11	Lost phones with client email are common	A setting in the device management console

A worked example: a Coimbatore textile exporter

A 300-employee Coimbatore textile exporter (fictional) had 45 office users, a factory floor with shared terminals, an ERP hosted by a local partner and buyers in Europe who had begun sending security questionnaires. Its IT team was two people.

The firm adopted IG1 as its target and used the buyers' questionnaires as a forcing date. It found that the factory terminals all used one shared login, that the ERP partner had a permanent VPN connection with no MFA, and that payroll spreadsheets sat in a folder open to every office user. In three months it gave each supervisor a named login, required MFA on the partner VPN (6.4) and wrote access requirements into the partner's contract, and restricted the payroll folder (3.3). It answered the buyers' questionnaires using its IG1 tracker as evidence, stating its status Safeguard by Safeguard rather than claiming any certification. Two buyers accepted the answers; one asked for an independent assessment, which the firm scheduled for the following year.

29.2 Start-ups: building it in from day one

A start-up has an advantage an older firm does not: there is little legacy to fix. A founding team that adopts a handful of habits in its first year can reach IG1 almost by default and IG2 with modest effort when enterprise customers begin to ask.

Habits that cost little at the start

- **Company-managed laptops from employee one,** enrolled in device management with encryption, screen lock, firewall and updates (3.6, 4.3, 4.5, 7.3).
- **Single sign-on and MFA for everything,** with joiners and leavers handled through the identity provider so that access is granted and revoked in one place (5.6, 6.1, 6.2, 6.3).
- **Infrastructure as code** for the cloud environment, so the configuration baseline is the code and every change is reviewed (4.1, 16.7).
- **Separate production and non-production** accounts or subscriptions from the start (16.8).
- **Dependency scanning in the build pipeline** and an inventory of third-party components (16.4, 16.5).
- **A public security contact** and a process to receive vulnerability reports (16.2).
- **Tenant audit logging on and retained** centrally from day one (8.2, 8.9, 8.10).

Product start-ups and Control 16

Control 16 has no IG1 Safeguards, which sometimes leads software start-ups to ignore it. That is a mistake for any firm whose product is software. A start-up whose customers rely on its application is, for those customers, a service provider, and its application security will be examined under their Control 15. Srida IT recommends that product start-ups treat 16.1, 16.2, 16.4, 16.5, 16.8 and 16.9 as part of their own baseline even while the rest of the organisation targets IG1.

A worked example: a Bengaluru SaaS start-up

A 25-person Bengaluru SaaS start-up (fictional) selling HR software to Indian mid-market firms was asked by its first large customer to complete a 200-question security assessment. Rather than answer question by question, the founders adopted IG1 as the company baseline and the six Control 16 Safeguards listed above for the product. They mapped the cus-

tomer's questions to Safeguards and answered from their tracker, attaching device compliance reports, the access review record and a summary of the dependency-scanning results. Because the product processed employee personal data, they also noted where their controls supported the customer's own DPDP Act safeguards, while making clear that the customer remained responsible as Data Fiduciary.

29.3 Managed service providers

Many SMEs outsource most of their IT to an MSP. That changes how the Controls apply but does not change who is accountable. The customer remains responsible for its own security; the MSP performs work on its behalf. At the same time, an MSP is a high-value target: one compromise of its remote management tools can reach every customer. MSPs therefore need to think about the CIS Controls in two ways.

1. The MSP's own environment

An MSP holds privileged access to dozens or hundreds of customer environments. For most MSPs that alone justifies treating their own environment at IG2, with selected IG3 Safeguards around privileged access: dedicated administrative workstations (12.8), centralised and recorded privileged access, strong MFA for every technician, service account inventory and review (5.5), monitoring and alerting on remote management platforms (13.1), and tested incident response with customer notification (17.4 to 17.8). The MSP's remote monitoring and management platform, documentation vault and ticketing system are its crown jewels and should be inventoried, hardened and logged accordingly.

2. Delivering the Controls for customers

An MSP can package the CIS Safeguards as services. The key is clarity about which Safeguards the MSP performs, which the customer performs and which are shared. A responsibility matrix, agreed in the contract, avoids the common failure where each party assumes the other is doing something.

Table 29-2. 2 — Example responsibility split for IG1 Safeguards between an SME customer and its MSP

Safeguards	MSP performs	Customer performs	Shared
1.1, 1.2	Maintains device register from management tools; weekly unknown-device check	Approves new devices; confirms owners	Annual reconciliation
2.1–2.3	Software inventory and support status report	Approves business software and exceptions	
3.1–3.5	Configures permissions, retention settings and disposal on request	Owns the data management process, data register and access decisions	Permission reviews
3.6, 4.3–4.7	Applies and reports on baseline settings	Approves the baseline and exceptions	
5.1–5.4, 6.1–6.5	Creates and removes accounts on instruction; enforces MFA	Requests and approves access; runs quarterly account review	Leaver process
7.1–7.4	Runs automated patching; reports compliance	Approves maintenance windows and risk acceptances	Remediation process
8.1–8.3	Enables logging and storage	Approves retention to meet legal obligations	
9.1, 9.2, 10.1–10.3	Deploys and monitors browser, DNS filtering and anti-malware controls	Reports suspicious activity	
11.1–11.4	Operates backups and isolated copy	Defines recovery priorities	Restore testing
12.1	Keeps network devices up to date		
14.1–14.8	May supply training content	Owns the programme and attendance	
15.1		Maintains service provider inventory, including the MSP	
17.1–17.3	Provides technical incident support and contact	Designates incident lead; owns regulatory reporting	Contact list and reporting process

The split shown is one example; real contracts vary. Note that some items always stay with the customer: approving risk, owning data, designating the incident lead and making regulatory notifications such as those under the CERT-In Directions or the DPDP Act. An MSP can help draft the notification, but the obligation sits with the customer.

Evidence from the MSP

When an SME is assessed, much of the evidence will come from the MSP's tools. The contract should require the MSP to supply, on request and at agreed intervals, reports such as device and software inventories, patch compliance, anti-malware status, backup job history, restore test results and account change logs. An MSP that cannot produce these is a finding against the customer's Control 15, and the customer's assessment will show many Safeguards as Partially implemented for lack of evidence.

Questions an SME should ask its MSP

- Which CIS Safeguards do you perform for us, and can we see the responsibility matrix?
- How do your technicians authenticate to our systems, and is MFA enforced on your remote management platform?
- Do your staff use named accounts in our environment, and do you remove access when a technician leaves?
- Where are our backups, who can delete them, and when did you last test a restore?
- How will you tell us about a security incident affecting your platform or ours, and how quickly?
- Where are our logs stored, and for how long?
- What reports will you give us each month that we can use as evidence?

29.4 India lens for small organisations

- The CERT-In Directions apply widely, including to many body corporates, so even small firms may have six-hour reporting and log retention duties. Confirm applicability and record the decision.
- Under the DPDP Act, an SME that decides why and how personal data is processed is a Data Fiduciary and must take reasonable security safeguards; an SME that processes data only on a client's instructions acts as a Data Processor under contract. The IG1 Safeguards give a defensible technical baseline for either role.
- SMEs that serve banks, insurers or listed companies will increasingly receive security clauses that flow down from RBI, IRDAI or SEBI requirements on their clients. A maintained IG1 tracker makes these requests much easier to answer.

29.5 Summary

For an SME, IG1 is achievable with existing tools and modest effort, and a few cheap IG2 Safeguards are worth adding early. For a start-up, the right habits in the first year make IG1 almost automatic and IG2 straightforward. For an MSP, the Controls are both a standard for its own high-risk environment and a menu of services, provided responsibilities and evidence are agreed in writing. In each case the result should be stated honestly as an assessed status against a target, never as a certification.

PART IV

Assessment

Running a CIS Controls assessment: scoping, choosing the Implementation Group, scoring, assessment techniques and evidence, findings, reporting and improvement.

CHAPTER 30

Running a CIS Controls Assessment

An assessment against the CIS Controls answers a simple question: for each Safeguard the enterprise should be doing, is it actually being done, and can that be shown? This chapter sets out how to plan and run such an assessment: agreeing its purpose, defining scope, choosing the target Implementation Group, applying the four-value evaluation scale consistently, and turning results into scores that mean something. Chapter 31 covers the testing techniques and evidence; Chapter 32 covers findings and reporting.

> **What an assessment is and is not.**
> A CIS Controls assessment is an evaluation of an enterprise's implementation of the Safeguards. It may be a self-assessment, an internal audit or an independent review. It is not a certification: CIS does not operate a scheme that certifies organisations against the Controls, and no assessment report should describe an enterprise as certified or compliant with them. Reports state the assessed status of each Safeguard at a point in time.

30.1 Step 1: agree the purpose

The purpose shapes everything else: the depth of testing, the independence required, the evidence standard and the audience for the report. Common purposes include:

- **Baseline:** a first view of where the enterprise stands, usually as a self-assessment, to plan a programme.
- **Progress check:** a repeat assessment to measure improvement against a previous baseline.
- **Assurance to the board or a regulator:** an internal audit or independent assessment with full testing and sampling.
- **Customer or supply-chain assurance:** evidence for a customer questionnaire or contract requirement.
- **Pre-audit readiness:** preparation for an ISO/IEC 27001 certification audit, a regulator's inspection or a CERT-In empanelled audit, using the CIS results as input.

Record the purpose in a short engagement document, together with the sponsor, the assessor or assessment team, the period under review, key dates and how disagreements about ratings will be resolved.

30.2 Step 2: define scope

Scope says which parts of the enterprise are covered. A vague scope ("the IT environment") produces arguments later about whether a finding counts. A good scope statement names:

- **Organisational units:** legal entities, business units, offices and plants.
- **Technology:** on-premises networks, data centres, cloud accounts and subscriptions, SaaS applications, OT networks, remote workers and personal devices used for work.
- **Third parties:** which service providers' activities are included, for example an MSP that administers the enterprise's endpoints.
- **Exclusions:** anything explicitly out of scope, with the reason. Exclusions must be disclosed in the report.
- **Period:** the time window for operating effectiveness, typically the last three, six or twelve months.

Scope can be narrower than the whole enterprise, for example a single product platform or the corporate network without the plants, but the report must say so clearly. A result for one subsidiary must not be presented as the group's result.

Scoping by asset class

CIS v8.1 organises Safeguards by asset class: devices, software, data, users, network and documentation. It is useful to list, for each class, what is in scope and roughly how large the population is. Population sizes drive sampling later. A scope table might show 420 end-user devices, 35 servers, 12 network devices, 3 cloud accounts, 140 SaaS applications, 610 user accounts, 48 service accounts and 22 service providers.

30.3 Step 3: choose the target Implementation Group

The target IG decides which Safeguards are tested. Chapter 3 and Chapter 26 discuss how to choose. In an assessment context, Srida IT applies these rules:

1. The target IG is decided by the enterprise's profile and risk, not by the result the enterprise hopes to achieve. An enterprise does not lower its target to improve its score.
2. If unsure, assess against IG1 for the whole scope and against IG2 for the higher-risk parts, then decide.
3. Selected higher-IG Safeguards may be added to the target, for example IG2 plus 1.5 and 15.5. List them explicitly.
4. Where a regulator or contract requires something that corresponds to a higher-IG Safeguard, include that Safeguard in scope regardless of the target IG.
5. The target IG and any additions are recorded before testing starts and approved by the sponsor.

Table 30-1. 1 — Typical target choices for fictional India-angle enterprises (Srida IT guidance)

Enterprise	Typical target	Safeguards in scope	Reasoning
40-person Kochi CA firm	IG1	56	Limited IT staff, client financial data, low exposure
300-employee Coimbatore textile exporter	IG1 plus 9.5, 11.5, 15.4	59	Small IT team; buyers ask about email fraud and supplier security
Bengaluru SaaS start-up	IG1 for the company; IG2 Control 16 for the product	56 plus 11	Customers rely on the application
600-employee Pune NBFC	IG2 plus 15.5, 15.6, 18.5	133	Regulated, sensitive financial data, IT team
Hyderabad hospital chain	IG2 plus 1.5, 3.14, 12.8, 15.5–15.7	136	Patient data, medical devices, many clinical vendors
Chennai auto-parts maker with OT	IG2 plus 1.5, 12.8, 13.8 for OT	133	OT safety and availability risk

The counts assume no Safeguards are Not applicable. In practice some will be, which reduces the number tested.

30.4 Step 4: plan the fieldwork

For each Safeguard in scope, the plan identifies the testing procedures from the relevant Control chapter, the people to interview, the systems to examine and the samples to draw. A practical planning sequence is:

1. Send an evidence request list in advance, grouped by Control, based on the documentation and evidence sections of Part II.
2. Hold an opening meeting to confirm scope, target IG, timetable, contacts and how evidence will be shared securely.
3. Review documents first: the Govern Safeguards (processes, policies, inventories) tell the assessor what the enterprise says it does.
4. Schedule interviews and system walk-throughs by Control owner rather than by Safeguard, to avoid repeated meetings.
5. Draw samples once populations are confirmed.
6. Book a closing meeting to discuss draft ratings before the report is issued.

A self-assessment for a 40-person firm can be done in two or three days of effort spread over a few weeks. An independent IG2 assessment of a mid-sized enterprise typically needs several weeks of fieldwork. The effort depends far more on the quality of the enterprise's own records than on its size.

30.5 Step 5: rate each Safeguard

Every Safeguard in scope receives one of four ratings, the same scale used throughout this manual.

Table 30-2. 2 — The evaluation scale applied to each Safeguard

Rating	Meaning	Typical evidence pattern
Implemented	The Safeguard is designed appropriately, covers the whole in-scope population, operates at the stated frequency throughout the review period, and is supported by evidence	Documented process matches practice; samples show no material exceptions; recurring activities happened on schedule
Partially implemented	The Safeguard exists but falls short in design, coverage, frequency or evidence in a way that leaves meaningful risk	Process exists but is not documented; coverage is incomplete; some cycles missed; evidence for part of the period only
Not implemented	The Safeguard is absent, or so incomplete that it provides no meaningful protection	No process, no tool, or a tool deployed but not configured or used
Not applicable	The Safeguard does not apply because the relevant asset, activity or condition does not exist in scope	Documented reason, accepted by the assessor and sponsor, revisited at the next assessment

Rules for consistent rating

- **Design and operation both count.** A well-written process that is not followed is at best Partially implemented. A practice that works but is not documented is also Partially implemented where the Safeguard calls for documentation.
- **Coverage matters.** Anti-malware on 92 per cent of endpoints is not Implemented. Decide in advance a tolerance for coverage exceptions (Srida IT suggests that any exception without a recorded, current justification prevents an Implemented rating) and apply it consistently.
- **Frequency is tested.** Where a Safeguard sets a cycle, such as weekly handling of unauthorised assets or quarterly account review, look for evidence of every cycle in the review period. Missing one cycle in twelve may still be Implemented with a note; missing several is Partially implemented.
- **Evidence is required.** "We do this" without evidence cannot be rated Implemented. In a self-assessment it should be rated Partially implemented with an action to produce evidence.
- **Compensating measures** may support a Partially implemented rating, or occasionally Implemented where they achieve the Safeguard's intent equally well. The reasoning must be recorded.
- **Not applicable is earned.** Common valid N/A cases are Control 16 Safeguards where the enterprise develops no software, or 4.11 and 4.12 where no portable devices hold enterprise data. "We have not got round to it" is Not implemented, not N/A.

30.6 Step 6: calculate scores

Ratings should always be reported Safeguard by Safeguard, because a single number hides which gaps matter. Summary scores are still useful for boards and for tracking progress. Srida IT uses the following method.

1. **Exclude N/A** Safeguards from the denominator and report how many were excluded.
2. **Coverage score** = number Implemented ÷ number in scope (excluding N/A), as a percentage.
3. **Weighted score** = (Implemented × 1 + Partially implemented × 0.5) ÷ number in scope, as a percentage. The half-weight for partial implementation is a convention and should be stated in the report.
4. **Report by IG and by Control.** Show IG1 results separately even when the target is IG2, since IG1 gaps are the most urgent.
5. **Never mix with maturity.** If the Srida IT maturity indicators are also assessed, report them separately (see Chapter 26).

Table 30-3. 3 — Example score calculation for an IG1 self-assessment

Item	Count
IG1 Safeguards	56
Not applicable	2
In scope	54
Implemented	41
Partially implemented	9
Not implemented	4

Item	Count
Coverage score (41 ÷ 54)	75.9%
Weighted score ((41 + 4.5) ÷ 54)	84.3%

Scores should not be used as targets in isolation. A 90 per cent weighted score with Not implemented ratings on backups and MFA is worse, in risk terms, than an 80 per cent score with gaps in documentation. Chapter 32 explains how to prioritise findings by risk rather than by count.

30.7 Tools for recording the assessment

A spreadsheet with one row per Safeguard, columns for rating, rationale, evidence references, testing procedures performed and actions, is adequate for most assessments. Appendix D provides an implementation status worksheet in that format, and Appendix H shows a completed workpaper.

CIS offers the **CIS Controls Self Assessment Tool (CSAT)**, a web-based application for tracking implementation of the Controls, with a hosted version and, for some users, an on-premises edition. Check its current availability, licensing terms, features and scoring scheme before relying on it. CSAT's own scoring approach may differ from the four-value scale used in this manual; if both are used, keep a mapping between them so that results remain comparable from year to year. The **CIS Controls Navigator** can help identify Safeguards and their mappings to other frameworks during planning.

30.8 Independence and objectivity

Self-assessments are valuable and are often the only practical option for small firms. Their limitation is that the people rating the Safeguards are the people running them. To strengthen a self-assessment:

- have a different person, even from another department, review a sample of ratings and their evidence;
- require evidence for every Implemented rating;
- record who performed the assessment and their relationship to each Control.

For board or regulatory assurance, an internal audit function or an independent assessor should perform or review the work. Where a regulator or contract requires an audit by a CERT-In empanelled auditor, the CIS assessment does not substitute for it, though it will make that audit faster.

30.9 India lens on assessment planning

- Plan to test the Indian-specific parameters alongside the Safeguards: 180-day log retention, time synchronisation sources and the six-hour reporting route under the CERT-In Directions.
- Where personal data is in scope, include the safeguards and breach intimation steps relevant to the DPDP Act 2023 and Rules 2025, and note that the assessment itself involves processing personal data (account lists, logs), which should be handled under appropriate confidentiality terms.
- For regulated entities, align the assessment period and evidence with the regulator's own audit cycle where practical, so that one set of evidence serves both.

30.10 A worked example

A 600-employee Pune NBFC (fictional) commissioned its internal audit team to assess the CIS Controls ahead of an RBI inspection. The engagement document set the purpose as assurance to the audit committee, the scope as the corporate network, data centre, two cloud subscriptions and the loan-origination SaaS platform, and the review period as the last six months. The plants of a sister company were explicitly excluded.

The target was IG2 plus 15.5, 15.6 and 18.5, giving 133 Safeguards. Four were rated N/A with recorded reasons, mostly in Control 16 where the NBFC used configured SaaS rather than in-house code, although 16.7 and 16.8 remained in scope for its integration scripts. Of the 129 in scope, 88 were Implemented, 31 Partially implemented and 10 Not implemented, giving a coverage score of 68.2 per cent and a weighted score of 80.2 per cent. The IG1 subset scored higher, with two

Partially implemented and no Not implemented ratings. The report led with the ten Not implemented Safeguards, ranked by risk, rather than with the percentages.

CHAPTER 31

Assessment Techniques and Evidence

A rating is only as good as the evidence behind it. This chapter explains the six testing methods used in the procedures throughout Part II, how to choose between them, how to sample, what good evidence looks like for different kinds of Safeguard, and how to record work so that another assessor could reach the same conclusion. The approach follows established audit practice, adapted to the specific, often technical, nature of the CIS Safeguards.

31.1 The six testing methods

Every testing procedure in this manual is labelled with one of six methods. They are complementary: most Safeguards need at least two to reach a reliable rating.

Table 31-1. 1 — Testing methods used in this manual

Method	What the assessor does	Strength	Limitation	Example
Examine	Reads documents, records, reports and configurations	Shows design and, for records, history	Documents can be out of date or describe intent rather than practice	Reading the vulnerability management process (7.1) and its review history
Interview	Asks the people responsible how the Safeguard works	Reveals understanding, workarounds and undocumented practice	Weakest evidence on its own; must be corroborated	Asking the service desk lead how a leaver's access is removed (6.2)
Observe	Watches the activity being performed	Direct evidence that the process happens as described	Point-in-time; people behave differently when watched	Watching an administrator log on with MFA to the firewall (6.5)
Inspect	Looks directly at a system, setting or asset	Strong evidence of current state	Shows today, not the review period	Checking the screen-lock policy on a sample laptop (4.3)
Re-perform	Independently carries out the control or a step of it	Strongest evidence of effectiveness	Time-consuming; needs access and skill	Running a discovery scan and comparing results with the asset register (1.1)
Sample	Selects items from a population and tests each	Supports conclusions about the whole population over a period	Conclusions limited by sample design	Selecting 25 leavers from the period and checking account disablement dates (5.3, 6.2)

Combining methods

A sound sequence for most Safeguards is: examine the documented process; interview the owner to understand how it works in practice; inspect or observe the current state; then sample over the review period to test operation. For technical Safeguards, re-performance often gives the most confidence for the least argument. For example, for 1.1 the assessor can run a discovery scan of one subnet and compare it with the register; for 9.2 the assessor can attempt to resolve a known test domain from a sampled endpoint and confirm it is blocked.

31.2 Design versus operating effectiveness

Two questions are asked of every Safeguard.

- **Design:** if the control works as described, would it achieve the Safeguard's intent across the whole scope? Tested mainly by examination and interview.
- **Operating effectiveness:** did it actually work that way throughout the review period? Tested mainly by inspection, sampling and re-performance.

A Safeguard with a design gap cannot be Implemented however well it operates within its limited design. A Safeguard with good design but missing operating evidence is at best Partially implemented. In a first-time baseline assessment, it is ac-

ceptable to rely more on design and current-state inspection, with a clear statement in the report that operating effectiveness over a period was not tested.

31.3 Sampling

Sampling allows an assessor to reach a conclusion about a population without testing every item. The CIS Safeguards produce two kinds of population: **assets or accounts** (devices, servers, users, providers) and **occurrences of a recurring activity** (weekly reviews, monthly patch cycles, backup jobs).

Sample sizes

Srida IT uses the following guideline sample sizes for non-statistical attribute sampling. They are consistent with common audit practice but are not prescribed by CIS. Larger samples are appropriate where the risk is higher or early results show exceptions.

Table 31-2. 2 — Guideline sample sizes for CIS Controls testing (Srida IT guidance)

Population or frequency	Population size or occurrences per year	Guideline sample
Annual activity	1	1 (the occurrence in the period)
Quarterly activity	4	2 (or all in the review period if shorter)
Monthly activity	12	2 to 4
Weekly activity	52	5 to 10
Daily or continuous activity	365 or more	20 to 40
Assets or accounts	Fewer than 50	All, or at least 10
Assets or accounts	50 to 250	15 to 25
Assets or accounts	More than 250	25 to 40, or use automated whole-population analysis

Selecting the sample

- Select from a **complete population** supplied by the system, not from a list prepared by the control owner. Check completeness by comparing totals with another source.
- Use **random or systematic selection**, with some deliberate selection of higher-risk items such as administrator accounts, internet-facing servers or providers holding sensitive data.
- Spread occurrence samples across the **whole review period**, including holiday periods and year-end, when controls often slip.
- Record the population, its source, the selection method and the items chosen.

Whole-population testing

Many CIS Safeguards are well suited to testing every item with a query or script, which is stronger than sampling. Examples include comparing all endpoints in the management console with the asset register (1.1), listing all accounts with no logon in 45 days (5.3), checking every device's patch level against the monthly deadline (7.3), or confirming that every in-scope server forwards logs to the central collector (8.9). Where whole-population analysis is used, the assessor should validate the query logic and the completeness of the data source.

Handling exceptions

When a sampled item fails, find out why. A single exception with a clear, isolated cause may be noted without changing the rating. Exceptions that suggest a systematic problem, such as several leavers whose accounts were disabled weeks late, should lead to an expanded sample or a Partially implemented rating. Never replace a failed sample item with another to avoid reporting the exception.

31.4 Evidence: what good looks like

Good evidence is **relevant** (it relates to the Safeguard being tested), **reliable** (produced by a system or an independent source rather than created for the assessment), **sufficient** (enough to support the conclusion across scope and period) and **dated** (it shows when it was produced and what period it covers).

Table 31-3. 3 — Evidence types and their relative reliability

Evidence type	Reliability	Notes
System-generated report or log extract, obtained by the assessor directly	High	Best evidence for operating effectiveness
Assessor's own inspection or re-performance results	High	Record the steps so they can be repeated
System-generated report supplied by the control owner	Medium to high	Check that it has not been edited, for example by re-running a sample
Approved, version-controlled document	Medium	Good evidence of design; not of operation
Ticket, email or meeting record	Medium	Useful for approvals and reviews if dated and attributable
Screenshot	Low to medium	Should show date, system and context; easily staged
Spreadsheet prepared by the control owner	Low to medium	Verify against the source system
Verbal statement	Low	Must be corroborated

Evidence by Safeguard type

The CIS Safeguards fall into a few recurring patterns, each with typical evidence.

- **Process Safeguards** (most Govern Safeguards, such as 3.1, 4.1, 7.1, 8.1, 11.1, 17.3): an approved document that covers the elements the Safeguard requires, with a review date within the last year, plus evidence that practice follows it.
- **Inventory Safeguards** (1.1, 2.1, 3.2, 5.1, 5.5, 6.6, 15.1, 16.4): the register itself, showing the required fields, an owner, a review date and evidence of reconciliation with a technical source.
- **Configuration Safeguards** (4.3 to 4.12, 9.1, 10.2, 10.3, 12.6): the baseline or policy, the management tool configuration and inspection of a sample of assets.
- **Recurring activity Safeguards** (1.2, 2.2, 5.3, 7.3, 7.4, 7.5, 7.6, 8.11, 11.2, 11.5, 12.1): records of each occurrence over the period, sampled.
- **People Safeguards** (14.1 to 14.9, 16.9, 17.1, 17.5): training content, attendance or completion records, role assignments and, where relevant, interviews to confirm understanding.
- **Testing Safeguards** (17.7, 18.2, 18.5, 16.13): reports from exercises and tests, with tracked remediation of findings.

31.5 Interviewing well

Interviews are where assessors learn how things really work. Each Control chapter in Part II suggests questions; the following practices make interviews more productive.

- Interview the person who does the work, not only the manager. Ask them to show rather than describe.
- Ask open questions: "Walk me through what happened the last time someone left the company" rather than "Do you disable leavers' accounts?"
- Ask about exceptions: "When did this not work?" and "What do you do when the tool is unavailable?"
- Note who said what, and corroborate important statements with evidence.
- In small firms, the same person may own many Controls. Group the questions to respect their time.

31.6 Technical testing safely

Re-performance and inspection often involve running tools on production systems. Agree the rules in advance: which tools, which systems, at what times, with whose approval, and who to call if something goes wrong. Avoid active scanning of OT networks or fragile medical devices without the system owner's explicit agreement; passive methods or vendor-supported checks are safer. Use read-only accounts where possible, and never use the enterprise's own administrator credentials without written authorisation. Any test that could disrupt service belongs in the penetration testing programme (Control 18), not in a controls assessment.

31.7 Recording the work

Every Control should have a workpaper, numbered WP-C01 to WP-C18, that records:

- the Safeguards in scope and any N/A decisions with reasons;
- each testing procedure performed, its method, the date and the assessor;
- populations, samples and results, including exceptions;
- evidence references, stored in a controlled location;
- the rating for each Safeguard and the reasoning;
- findings raised, cross-referenced to the findings register (Chapter 32);
- reviewer sign-off.

Appendix H shows a completed workpaper. The test of a good workpaper is that a second, competent assessor reading it would understand what was done and reach the same rating.

31.8 Handling evidence securely

Assessment evidence often contains sensitive material: account lists, network diagrams, vulnerability scan results, configuration exports and logs that include personal data. Treat it as confidential:

- collect only what is needed, and redact personal data where it does not affect the test;
- store evidence in an access-controlled, encrypted location;
- agree a retention period and delete evidence at the end of it;
- under the DPDP Act 2023, an external assessor processing personal data on the enterprise's behalf may be acting as a Data Processor, and the engagement terms should reflect that.

31.9 India lens: testing local parameters

Table 31-4. 4 — Example tests for Indian regulatory parameters linked to the Safeguards

Parameter	Related Safeguards	Example test
180-day log retention within India under the CERT-In Directions	8.1, 8.3, 8.10	Inspect retention settings on the log platform and retrieve a log entry from about 170 days ago; confirm the storage region
Clock synchronisation to designated sources	8.4	Inspect time configuration on a sample of servers and network devices; compare clock offsets
Six-hour incident reporting	17.2, 17.3, 17.4	Examine the procedure for the reporting clock; sample reported incidents and compare detection and report times
Point of contact designated to CERT-In	17.1, 17.2	Examine the designation and confirm the contact details are current
Personal data breach intimation under the DPDP Rules 2025	17.3, 17.4, 17.6	Examine the procedure for notifying the Board and Data Principals; check templates exist

31.10 A worked example

An assessor testing Control 5 at a Hyderabad hospital chain (fictional) received a user list of 2,140 accounts from the HR team. Before sampling, she compared it with a directory export and found 2,310 accounts; the difference was mostly contractors and service accounts that HR did not track. She used the directory export as the population. A whole-population query found 186 enabled accounts with no logon in more than 45 days (5.3), of which 61 belonged to people who had left. She then sampled 25 leavers from the six-month period: 19 had accounts disabled within a day, four within a week and two remained enabled. Interviews revealed that agency nursing staff were not passed through the HR leaver process. The rating for 5.3 was Not implemented because there was no automated control on dormant accounts at all; 6.2 was rated Partially implemented because a leaver process existed and mostly worked but failed for a whole category of staff. Both findings recorded the population source, the queries used and the evidence references.

CHAPTER 32

Findings, Reporting and Improvement

An assessment earns its cost only if it leads to change. This chapter covers how to write findings that people will act on, how to rank them by risk rather than by count, how to report to different audiences without overstating or understating the position, and how to turn results into an improvement cycle that is measured and sustained. It closes with guidance on re-assessment and on avoiding the claims that the CIS Controls do not support.

32.1 Writing a finding

A finding records a gap between what a Safeguard expects and what the assessor found. Srida IT uses the Condition – Criteria – Cause – Effect – Recommendation structure, familiar from internal audit, because it forces the writer to explain why the gap matters and what to do about it.

Table 32-1. 1 — Structure of a finding

Element	Question it answers	Example (Safeguard 11.4)
Condition	What did we find?	Backups of the file server and ERP database are written to a storage appliance on the production network, reachable with the same domain administrator credentials used for daily administration. No offline or logically isolated copy exists.
Criteria	What should be the case?	Safeguard 11.4 expects at least one instance of recovery data to be kept isolated from the production environment. The enterprise's data recovery process (11.1) also states that an offline copy will be maintained.
Cause	Why did it happen?	The tape rotation was retired when the appliance was installed and no replacement isolation was designed.
Effect	What could go wrong?	An attacker with domain administrator access, a common step in ransomware attacks, could delete or encrypt both production data and all backups, preventing recovery.
Recommendation	What should be done?	Establish an isolated copy (immutable storage, a separate administrative domain or offline media) within 30 days; update 11.1 to describe it; add it to quarterly restore testing.

Good practice in writing findings

- **One finding per root cause,** not per Safeguard. If missing MFA affects 6.3, 6.4 and 6.5 for the same reason, write one finding and reference all three.
- **Be specific.** "Some servers are not patched" is not a finding. "Seven of 35 servers, including both internet-facing web servers, were more than 60 days behind on operating system updates at the date of testing" is.
- **Quote evidence references,** so the finding can be traced to the workpaper.
- **Avoid blame.** Findings describe systems and processes, not individuals.
- **Separate fact from opinion.** The condition is fact; the effect is a reasoned judgement; the recommendation is advice.
- **Agree the facts** with the control owner before the report is issued. Disagreement about the recommendation is acceptable; disagreement about the condition should be resolved.

32.2 Rating findings by risk

Counting Not implemented Safeguards is a poor guide to priority. A missing data classification scheme (3.7) and missing backups (11.2) are each one Safeguard, but the second can end the business. Srida IT rates each finding on a four-level scale considering the likelihood that the gap will be exploited or cause harm and the impact if it does.

Table 32-2. 2 — Finding risk ratings (Srida IT scale)

Rating	Description	Typical examples	Expected response

Rating	Description	Typical examples	Expected response
Critical	A gap that is actively exploited by common attacks and could cause severe or irreversible harm	No MFA on email or remote access; no isolated backup; internet-facing systems unpatched for months; shared administrator accounts	Immediate action; interim mitigation within days; executive owner
High	A significant gap likely to contribute to a serious incident	Incomplete asset inventory; dormant accounts not disabled; no log collection on key systems; no incident contacts	Remediation plan within 30 days, completion within 90
Medium	A gap that weakens defence in depth or detection	Process documents not reviewed; training not covering all topics; inconsistent software support review	Remediation within six months
Low	A gap in documentation or efficiency with little direct risk	Register fields incomplete; evidence not retained in a consistent way	Address in the normal improvement cycle

Two further factors should raise a rating. First, any IG1 gap in an enterprise targeting IG2 or IG3 signals that the foundations are weak. Second, any gap that also breaches an Indian legal or regulatory obligation, such as missing log retention under the CERT-In Directions or no breach intimation route under the DPDP Rules, carries regulatory exposure as well as security risk.

32.3 The findings register

All findings go into a single register that outlives the assessment. Each row records the finding ID, the Safeguards affected, the risk rating, the owner, the agreed action, the target date, status and closure evidence. Appendix E provides a gap analysis and 12-month action plan template in this form.

Closure must be evidenced. A finding is closed when the assessor or an independent reviewer has seen evidence that the action is complete and effective, not when the owner says it is done. For Critical and High findings, Srida IT recommends a short retest before closure.

32.4 Reporting to different audiences

The full assessment report

The full report is for the sponsor, control owners and, where relevant, internal audit or the regulator. A typical structure is:

1. **Executive summary:** purpose, scope, target IG, overall conclusion, the most important findings and the scores, in two pages or fewer.
2. **Scope and approach:** what was covered and excluded, the review period, methods and sampling, limitations.
3. **Results by Control:** a table of every Safeguard with its rating, and a short narrative per Control.
4. **Findings:** each finding in the structure above, ordered by risk.
5. **Not applicable decisions:** every N/A with its reason.
6. **Regulatory observations:** where findings touch Indian obligations, with a clear statement that the assessment is not a legal compliance opinion.
7. **Management responses:** agreed actions, owners and dates.
8. **Appendices:** workpaper index, evidence list, scoring method.

The board report

Boards need a short, honest picture: where the enterprise stands against its target, the few things that matter most, what is being done and whether it is on track. Appendix I provides a one-page template. Srida IT recommends:

- stating the target IG and why it was chosen;
- showing coverage and weighted scores for IG1 and for the target IG, with the trend from the last assessment;
- listing Critical and High findings in plain language, each with owner and date;
- showing maturity separately from IG coverage, if maturity is assessed;
- highlighting any risk the board is being asked to accept.

Table 32-3. 3 — Example board dashboard summary

Measure	Last assessment	This assessment	Target by next assessment
IG1 coverage score	78%	93%	100%
IG2 (target) coverage score	51%	68%	80%
IG2 weighted score	66%	80%	88%
Open Critical findings	4	1	0
Open High findings	11	7	3
Findings past target date	6	2	0

Customers and third parties

Customers often ask for evidence of security practice. A summary letter or extract can share the scope, target IG, assessment date, the assessor's identity and independence, and the overall status, with a commitment to remediate open items. It should not disclose detailed vulnerabilities. It must not describe the enterprise as certified or compliant against the CIS Controls, and it should not imply any endorsement by CIS. A suitable form of words is: “An assessment of our implementation of the CIS Critical Security Controls v8.1, Implementation Group 2, was completed in [month year] by [assessor]. Of 128 applicable Safeguards, 117 were assessed as implemented; remediation of the remainder is under way.”

32.5 Wording to avoid

Because CIS runs no scheme that certifies organisations, some wording misleads readers and should not appear in any report, marketing material or customer response.

Table 32-4. 4 — Misleading and accurate wording

Avoid	Use instead
"We are certified against the CIS Controls"	"We assess our security against the CIS Controls v8.1"
"We have achieved IG2"	"Our target is IG2; at our last assessment 92% of applicable IG2 Safeguards were implemented"
"Fully compliant with the CIS Controls"	"All applicable IG1 Safeguards were assessed as implemented on [date]"
"CIS-approved assessment"	"Assessment performed by [name] using the CIS Controls v8.1"
"Our CIS score proves we meet DPDP requirements"	"Our CIS implementation supports the security safeguards we maintain under the DPDP Act; compliance is assessed separately"

32.6 Turning results into improvement

The 12-month plan

After each assessment, convert the findings register into a 12-month plan with quarterly milestones. A practical ordering is:

1. **Quarter 1:** close or mitigate all Critical findings; start all High findings; fix any IG1 gaps.
2. **Quarter 2:** complete High findings; begin Medium findings that depend on tooling or budget decisions.
3. **Quarter 3:** complete Medium findings; start the next wave of target-IG Safeguards not yet implemented.
4. **Quarter 4:** close Low findings; run a self-check of the IG1 recurring activities; prepare for reassessment.

Each action needs an owner with authority to deliver it, a realistic date and, where it depends on spending, a budget decision. Actions without owners do not happen.

Root cause and recurrence

Where the same kind of finding recurs, for example missed review cycles across several Controls, look for a common cause. Often it is a lack of scheduling, ownership or tooling rather than individual failure. Fix the cause: a compliance cal-

endar with automatic reminders, a named owner for each recurring activity and a monthly check by the security lead will close many recurring findings at once.

Metrics between assessments

Annual assessments leave long gaps. A small set of operational metrics, reviewed monthly, shows whether the improvements are holding. Each Control chapter in Part II suggests metrics. A balanced set for most enterprises might include:

- percentage of devices in the register that reported to management tools in the last seven days;
- percentage of endpoints within the patching deadline;
- number of enabled accounts inactive for more than 45 days;
- percentage of users and administrators enrolled in MFA;
- days since the last successful restore test;
- number of open Critical and High findings, and the number past due.

32.7 Reassessment

Reassess at least annually, and after significant change: a merger, a major cloud migration, a serious incident or a change in regulatory status. Each reassessment should:

- retest IG1 in full, even if the target is higher;
- retest every Safeguard previously rated Partially implemented or Not implemented;
- revisit every N/A decision;
- retest a rotating sample of Safeguards previously rated Implemented, so that over two or three years every Safeguard is retested;
- compare scores with the previous assessment using the same method, and explain any change of method.

When CIS publishes a new version of the Controls, map the existing results to the new version and note which Safeguards changed. Do not carry ratings forward without checking that the Safeguard's expectation is still the same.

32.8 India lens on reporting

- For regulated entities, align the board report with the cyber security reporting the regulator expects from the board or its committees, so that one pack serves both.
- Where a finding reveals that a reportable incident may have occurred, such as evidence of compromise found during testing, escalate it through the incident process immediately rather than waiting for the report. CERT-In and DPDP timelines run from awareness, not from report issue.
- Keep assessment reports and evidence under confidentiality and record-retention rules consistent with the enterprise's obligations and any regulatory inspection needs.

32.9 A worked example

A 300-employee Coimbatore textile exporter (fictional) completed its first independent IG1 assessment with 44 of 55 applicable Safeguards Implemented. The assessor raised six findings. Two were Critical: the ERP partner's VPN without MFA (6.4) and backups without an isolated copy (11.4). Three were High: incomplete device inventory covering factory terminals (1.1, 1.2), no dormant-account control (5.3) and no incident contacts or reporting route (17.2, 17.3). One was Medium: awareness training that did not cover insecure networks or missing updates (14.7, 14.8).

The board report showed an IG1 coverage score of 80 per cent and listed the two Critical findings in a sentence each, with owners and 30-day dates. Both were closed and retested within five weeks. The High findings closed within the quarter. At the reassessment a year later, the firm rated 54 of 55 Safeguards Implemented, with one Partially implemented item on software support review, and decided to add DMARC and quarterly restore testing from IG2. Its customer letter stated the assessment scope, date, assessor and result, without any claim of certification.

PART V

Appendices and Templates

Safeguard and Control matrices, an IG1 self-assessment checklist, implementation status and gap analysis templates, the CIS–ISO/IEC 27001 crosswalk, the India regulatory touchpoints matrix, a completed workpaper, a board reporting template and references.

APPENDIX A

Safeguard Matrix

All 153 Safeguards of CIS Controls v8.1 with the CIS title, asset type, security function and the lowest Implementation Group that includes them, and the testing procedures in Part II that address them. Titles and attributes © Center for Internet Security, CC BY-NC-ND 4.0; see cisecurity.org/controls for the authoritative text.

Table A-1. Safeguard matrix

Safeguard	Title (CIS wording)	Asset type	Function	From	Testing procedures
1.1	“Establish and Maintain Detailed Enterprise Asset Inventory”	Devices	Identify	**IG1**	TP-C01-01, TP-C01-02, TP-C01-03, TP-C01-10
1.2	“Address Unauthorized Assets”	Devices	Respond	**IG1**	TP-C01-04, TP-C01-05
1.3	“Utilize an Active Discovery Tool”	Devices	Detect	**IG2**	TP-C01-06
1.4	“Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory”	Devices	Identify	**IG2**	TP-C01-07, TP-C01-08
1.5	“Use a Passive Asset Discovery Tool”	Devices	Detect	**IG3**	TP-C01-09
2.1	“Establish and Maintain a Software Inventory”	Software	Identify	**IG1**	TP-C02-01, TP-C02-02, TP-C02-11
2.2	“Ensure Authorized Software is Currently Supported”	Software	Identify	**IG1**	TP-C02-03, TP-C02-04
2.3	“Address Unauthorized Software”	Software	Respond	**IG1**	TP-C02-05
2.4	“Utilize Automated Software Inventory Tools”	Software	Detect	**IG2**	TP-C02-06
2.5	“Allowlist Authorized Software”	Software	Protect	**IG2**	TP-C02-07, TP-C02-08
2.6	“Allowlist Authorized Libraries”	Software	Protect	**IG2**	TP-C02-09
2.7	“Allowlist Authorized Scripts”	Software	Protect	**IG3**	TP-C02-10
3.1	“Establish and Maintain a Data Management Process”	Data	Govern	**IG1**	TP-C03-01, TP-C03-02
3.2	“Establish and Maintain a Data Inventory”	Data	Identify	**IG1**	TP-C03-03, TP-C03-04
3.3	“Configure Data Access Control Lists”	Data	Protect	**IG1**	TP-C03-05, TP-C03-06
3.4	“Enforce Data Retention”	Data	Protect	**IG1**	TP-C03-07, TP-C03-08
3.5	“Securely Dispose of Data”	Data	Protect	**IG1**	TP-C03-09, TP-C03-10
3.6	“Encrypt Data on End-User Devices”	Data	Protect	**IG1**	TP-C03-11
3.7	“Establish and Maintain a Data Classification Scheme”	Data	Identify	**IG2**	TP-C03-12, TP-C03-13
3.8	“Document Data Flows”	Data	Identify	**IG2**	TP-C03-14
3.9	“Encrypt Data on Removable Media”	Data	Protect	**IG2**	TP-C03-15
3.10	“Encrypt Sensitive Data in Transit”	Data	Protect	**IG2**	TP-C03-16
3.11	“Encrypt Sensitive Data at Rest”	Data	Protect	**IG2**	TP-C03-17
3.12	“Segment Data Processing and Storage Based on Sensitivity”	Data	Protect	**IG2**	TP-C03-18
3.13	“Deploy a Data Loss Prevention Solution”	Data	Protect	**IG3**	TP-C03-19, TP-C03-20
3.14	“Log Sensitive Data Access”	Data	Detect	**IG3**	TP-C03-21, TP-C03-22
4.1	“Establish and Maintain a Secure Configuration Process”	Documentation	Govern	**IG1**	TP-C04-01, TP-C04-02, TP-C04-17
4.2	“Establish and Maintain a Secure Configuration Process for Network Infrastructure”	Documentation	Govern	**IG1**	TP-C04-03, TP-C04-04
4.3	“Configure Automatic Session Locking on Enterprise Assets”	Devices	Protect	**IG1**	TP-C04-05, TP-C04-06
4.4	“Implement and Manage a Firewall on Servers”	Devices	Protect	**IG1**	TP-C04-07
4.5	“Implement and Manage a Firewall on End-User Devices”	Devices	Protect	**IG1**	TP-C04-08

Safeguard	Title (CIS wording)	Asset type	Function	From	Testing procedures
4.6	“Securely Manage Enterprise Assets and Software”	Devices	Protect	**IG1**	TP-C04-09, TP-C04-10
4.7	“Manage Default Accounts on Enterprise Assets and Software”	Users	Protect	**IG1**	TP-C04-11
4.8	“Uninstall or Disable Unnecessary Services on Enterprise Assets and Software”	Devices	Protect	**IG2**	TP-C04-12
4.9	“Configure Trusted DNS Servers on Enterprise Assets”	Devices	Protect	**IG2**	TP-C04-13
4.10	“Enforce Automatic Device Lockout on Portable End-User Devices”	Devices	Protect	**IG2**	TP-C04-14
4.11	“Enforce Remote Wipe Capability on Portable End-User Devices”	Data	Protect	**IG2**	TP-C04-15
4.12	“Separate Enterprise Workspaces on Mobile End-User Devices”	Data	Protect	**IG3**	TP-C04-16
5.1	“Establish and Maintain an Inventory of Accounts”	Users	Identify	**IG1**	TP-C05-01, TP-C05-02, TP-C05-03, TP-C05-14
5.2	“Use Unique Passwords”	Users	Protect	**IG1**	TP-C05-04, TP-C05-05
5.3	“Disable Dormant Accounts”	Users	Protect	**IG1**	TP-C05-06, TP-C05-07
5.4	“Restrict Administrator Privileges to Dedicated Administrator Accounts”	Users	Protect	**IG1**	TP-C05-08, TP-C05-09
5.5	“Establish and Maintain an Inventory of Service Accounts”	Users	Identify	**IG2**	TP-C05-10, TP-C05-11
5.6	“Centralize Account Management”	Users	Govern	**IG2**	TP-C05-12, TP-C05-13
6.1	“Establish an Access Granting Process”	Documentation	Govern	**IG1**	TP-C06-01, TP-C06-02
6.2	“Establish an Access Revoking Process”	Documentation	Govern	**IG1**	TP-C06-03, TP-C06-04
6.3	“Require MFA for Externally-Exposed Applications”	Users	Protect	**IG1**	TP-C06-05, TP-C06-06
6.4	“Require MFA for Remote Network Access”	Users	Protect	**IG1**	TP-C06-07
6.5	“Require MFA for Administrative Access”	Users	Protect	**IG1**	TP-C06-08, TP-C06-13
6.6	“Establish and Maintain an Inventory of Authentication and Authorization Systems”	Software	Identify	**IG2**	TP-C06-09
6.7	“Centralize Access Control”	Users	Protect	**IG2**	TP-C06-10
6.8	“Define and Maintain Role-Based Access Control”	Users	Govern	**IG3**	TP-C06-11, TP-C06-12
7.1	“Establish and Maintain a Vulnerability Management Process”	Documentation	Govern	**IG1**	TP-C07-01, TP-C07-02
7.2	“Establish and Maintain a Remediation Process”	Documentation	Govern	**IG1**	TP-C07-03, TP-C07-04
7.3	“Perform Automated Operating System Patch Management”	Software	Protect	**IG1**	TP-C07-05, TP-C07-06
7.4	“Perform Automated Application Patch Management”	Software	Protect	**IG1**	TP-C07-07
7.5	“Perform Automated Vulnerability Scans of Internal Enterprise Assets”	Software	Identify	**IG2**	TP-C07-08, TP-C07-09
7.6	“Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets”	Software	Identify	**IG2**	TP-C07-10, TP-C07-11
7.7	“Remediate Detected Vulnerabilities”	Software	Respond	**IG2**	TP-C07-12, TP-C07-13
8.1	“Establish and Maintain an Audit Log Management Process”	Documentation	Govern	**IG1**	TP-C08-01, TP-C08-02
8.2	“Collect Audit Logs”	Data	Detect	**IG1**	TP-C08-03, TP-C08-04
8.3	“Ensure Adequate Audit Log Storage”	Data	Protect	**IG1**	TP-C08-05
8.4	“Standardize Time Synchronization”	Data	Protect	**IG2**	TP-C08-06, TP-C08-07
8.5	“Collect Detailed Audit Logs”	Data	Detect	**IG2**	TP-C08-08
8.6	“Collect DNS Query Audit Logs”	Data	Detect	**IG2**	TP-C08-09
8.7	“Collect URL Request Audit Logs”	Data	Detect	**IG2**	TP-C08-10
8.8	“Collect Command-Line Audit Logs”	Data	Detect	**IG2**	TP-C08-11
8.9	“Centralize Audit Logs”	Data	Detect	**IG2**	TP-C08-12, TP-C08-13
8.10	“Retain Audit Logs”	Data	Protect	**IG2**	TP-C08-14, TP-C08-15

Safeguard	Title (CIS wording)	Asset type	Function	From	Testing procedures
8.11	“Conduct Audit Log Reviews”	Data	Detect	**IG2**	TP-C08-16, TP-C08-17
8.12	“Collect Service Provider Logs”	Data	Detect	**IG3**	TP-C08-18
9.1	“Ensure Use of Only Fully Supported Browsers and Email Clients”	Software	Protect	**IG1**	TP-C09-01, TP-C09-02
9.2	“Use DNS Filtering Services”	Devices	Protect	**IG1**	TP-C09-03, TP-C09-04
9.3	“Maintain and Enforce Network-Based URL Filters”	Network	Protect	**IG2**	TP-C09-05, TP-C09-06
9.4	“Restrict Unnecessary or Unauthorized Browser and Email Client Extensions”	Software	Protect	**IG2**	TP-C09-07
9.5	“Implement DMARC”	Network	Protect	**IG2**	TP-C09-08, TP-C09-09
9.6	“Block Unnecessary File Types”	Network	Protect	**IG2**	TP-C09-10
9.7	“Deploy and Maintain Email Server Anti-Malware Protections”	Network	Protect	**IG3**	TP-C09-11
10.1	“Deploy and Maintain Anti-Malware Software”	Devices	Detect	**IG1**	TP-C10-01, TP-C10-02, TP-C10-03
10.2	“Configure Automatic Anti-Malware Signature Updates”	Devices	Protect	**IG1**	TP-C10-04, TP-C10-05
10.3	“Disable Autorun and Autoplay for Removable Media”	Devices	Protect	**IG1**	TP-C10-06, TP-C10-07
10.4	“Configure Automatic Anti-Malware Scanning of Removable Media”	Devices	Detect	**IG2**	TP-C10-08
10.5	“Enable Anti-Exploitation Features”	Devices	Protect	**IG2**	TP-C10-09
10.6	“Centrally Manage Anti-Malware Software”	Devices	Protect	**IG2**	TP-C10-10, TP-C10-11
10.7	“Use Behavior-Based Anti-Malware Software”	Devices	Detect	**IG2**	TP-C10-12, TP-C10-13, TP-C10-14
11.1	“Establish and Maintain a Data Recovery Process”	Documentation	Govern	**IG1**	TP-C11-01, TP-C11-02
11.2	“Perform Automated Backups”	Data	Recover	**IG1**	TP-C11-03, TP-C11-04
11.3	“Protect Recovery Data”	Data	Protect	**IG1**	TP-C11-05, TP-C11-06
11.4	“Establish and Maintain an Isolated Instance of Recovery Data”	Data	Recover	**IG1**	TP-C11-07, TP-C11-08
11.5	“Test Data Recovery”	Data	Recover	**IG2**	TP-C11-09, TP-C11-10, TP-C11-11, TP-C11-12
12.1	“Ensure Network Infrastructure is Up-to-Date”	Network	Protect	**IG1**	TP-C12-01, TP-C12-02
12.2	“Establish and Maintain a Secure Network Architecture”	Network	Protect	**IG2**	TP-C12-03, TP-C12-04
12.3	“Securely Manage Network Infrastructure”	Network	Protect	**IG2**	TP-C12-05, TP-C12-06
12.4	“Establish and Maintain Architecture Diagram(s)”	Documentation	Govern	**IG2**	TP-C12-07
12.5	“Centralize Network Authentication, Authorization, and Auditing (AAA)”	Network	Protect	**IG2**	TP-C12-08, TP-C12-09
12.6	“Use of Secure Network Management and Communication Protocols”	Network	Protect	**IG2**	TP-C12-10, TP-C12-11
12.7	“Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise’s AAA Infrastructure”	Devices	Protect	**IG2**	TP-C12-12, TP-C12-13
12.8	“Establish and Maintain Dedicated Computing Resources for All Administrative Work”	Devices	Protect	**IG3**	TP-C12-14, TP-C12-15
13.1	“Centralize Security Event Alerting”	Network	Detect	**IG2**	TP-C13-01, TP-C13-02, TP-C13-14
13.2	“Deploy a Host-Based Intrusion Detection Solution”	Devices	Detect	**IG2**	TP-C13-03
13.3	“Deploy a Network Intrusion Detection Solution”	Network	Detect	**IG2**	TP-C13-04, TP-C13-05
13.4	“Perform Traffic Filtering Between Network Segments”	Network	Protect	**IG2**	TP-C13-06
13.5	“Manage Access Control for Remote Assets”	Devices	Protect	**IG2**	TP-C13-07
13.6	“Collect Network Traffic Flow Logs”	Network	Detect	**IG2**	TP-C13-08
13.7	“Deploy a Host-Based Intrusion Prevention Solution”	Devices	Protect	**IG3**	TP-C13-09
13.8	“Deploy a Network Intrusion Prevention Solution”	Network	Protect	**IG3**	TP-C13-10

Safeguard	Title (CIS wording)	Asset type	Function	From	Testing procedures
13.9	“Deploy Port-Level Access Control”	Network	Protect	**IG3**	TP-C13-11
13.10	“Perform Application Layer Filtering”	Network	Protect	**IG3**	TP-C13-12
13.11	“Tune Security Event Alerting Thresholds”	Network	Detect	**IG3**	TP-C13-13
14.1	“Establish and Maintain a Security Awareness Program”	Documentation	Govern	**IG1**	TP-C14-01, TP-C14-02, TP-C14-11
14.2	“Train Workforce Members to Recognize Social Engineering Attacks”	Users	Protect	**IG1**	TP-C14-03
14.3	“Train Workforce Members on Authentication Best Practices”	Users	Protect	**IG1**	TP-C14-04
14.4	“Train Workforce on Data Handling Best Practices”	Users	Protect	**IG1**	TP-C14-05
14.5	“Train Workforce Members on Causes of Unintentional Data Exposure”	Users	Protect	**IG1**	TP-C14-06
14.6	“Train Workforce Members on Recognizing and Reporting Security Incidents”	Users	Protect	**IG1**	TP-C14-07
14.7	“Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates”	Users	Protect	**IG1**	TP-C14-08
14.8	“Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks”	Users	Protect	**IG1**	TP-C14-09
14.9	“Conduct Role-Specific Security Awareness and Skills Training”	Users	Protect	**IG2**	TP-C14-10
15.1	“Establish and Maintain an Inventory of Service Providers”	Users	Identify	**IG1**	TP-C15-01, TP-C15-02
15.2	“Establish and Maintain a Service Provider Management Policy”	Documentation	Govern	**IG2**	TP-C15-03
15.3	“Classify Service Providers”	Users	Govern	**IG2**	TP-C15-04
15.4	“Ensure Service Provider Contracts Include Security Requirements”	Documentation	Govern	**IG2**	TP-C15-05, TP-C15-06
15.5	“Assess Service Providers”	Users	Govern	**IG3**	TP-C15-07
15.6	“Monitor Service Providers”	Data	Govern	**IG3**	TP-C15-08
15.7	“Securely Decommission Service Providers”	Data	Protect	**IG3**	TP-C15-09, TP-C15-10
16.1	“Establish and Maintain a Secure Application Development Process”	Documentation	Govern	**IG2**	TP-C16-01, TP-C16-02, TP-C16-18
16.2	“Establish and Maintain a Process to Accept and Address Software Vulnerabilities”	Documentation	Govern	**IG2**	TP-C16-03, TP-C16-04
16.3	“Perform Root Cause Analysis on Security Vulnerabilities”	Software	Protect	**IG2**	TP-C16-05
16.4	“Establish and Manage an Inventory of Third-Party Software Components”	Software	Identify	**IG2**	TP-C16-06, TP-C16-07
16.5	“Use Up-to-Date and Trusted Third-Party Software Components”	Software	Protect	**IG2**	TP-C16-08
16.6	“Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities”	Documentation	Govern	**IG2**	TP-C16-09
16.7	“Use Standard Hardening Configuration Templates for Application Infrastructure”	Software	Protect	**IG2**	TP-C16-10
16.8	“Separate Production and Non-Production Systems”	Network	Protect	**IG2**	TP-C16-11
16.9	“Train Developers in Application Security Concepts and Secure Coding”	Users	Protect	**IG2**	TP-C16-12
16.10	“Apply Secure Design Principles in Application Architectures”	Software	Protect	**IG2**	TP-C16-13
16.11	“Leverage Vetted Modules or Services for Application Security Components”	Software	Identify	**IG2**	TP-C16-14
16.12	“Implement Code-Level Security Checks”	Software	Protect	**IG3**	TP-C16-15
16.13	“Conduct Application Penetration Testing”	Software	Detect	**IG3**	TP-C16-16
16.14	“Conduct Threat Modeling”	Software	Protect	**IG3**	TP-C16-17
17.1	“Designate Personnel to Manage Incident Handling”	Users	Respond	**IG1**	TP-C17-01, TP-C17-02

Safeguard	Title (CIS wording)	Asset type	Function	From	Testing procedures
17.2	“Establish and Maintain Contact Information for Reporting Security Incidents”	Documentation	Govern	**IG1**	TP-C17-03
17.3	“Establish and Maintain an Enterprise Process for Reporting Incidents”	Documentation	Govern	**IG1**	TP-C17-04
17.4	“Establish and Maintain an Incident Response Process”	Documentation	Govern	**IG2**	TP-C17-05, TP-C17-06
17.5	“Assign Key Roles and Responsibilities”	Users	Respond	**IG2**	TP-C17-07
17.6	“Define Mechanisms for Communicating During Incident Response”	Users	Respond	**IG2**	TP-C17-08
17.7	“Conduct Routine Incident Response Exercises”	Users	Recover	**IG2**	TP-C17-09, TP-C17-10
17.8	“Conduct Post-Incident Reviews”	Users	Recover	**IG2**	TP-C17-11
17.9	“Establish and Maintain Security Incident Thresholds”	Documentation	Recover	**IG3**	TP-C17-12
18.1	“Establish and Maintain a Penetration Testing Program”	Documentation	Govern	**IG2**	TP-C18-01, TP-C18-02
18.2	“Perform Periodic External Penetration Tests”	Network	Detect	**IG2**	TP-C18-03, TP-C18-04
18.3	“Remediate Penetration Test Findings”	Network	Protect	**IG2**	TP-C18-05
18.4	“Validate Security Measures”	Network	Protect	**IG3**	TP-C18-06, TP-C18-07
18.5	“Perform Periodic Internal Penetration Tests”	Network	Detect	**IG3**	TP-C18-08, TP-C18-09

APPENDIX B

Control Summary

All 18 Controls with the number of Safeguards first introduced in each Implementation Group, the number of testing procedures, the chapter of Part II where they are covered and the workpaper reference.

Table B-1. Control summary

Control	Title	Safeguards	IG1	IG2 adds	IG3 adds	Tests	Chapter	Workpaper
1	Inventory and Control of Enterprise Assets	5	2	2	1	10	7	WP-C01
2	Inventory and Control of Software Assets	7	3	3	1	11	8	WP-C02
3	Data Protection	14	6	6	2	22	9	WP-C03
4	Secure Configuration of Enterprise Assets and Software	12	7	4	1	17	10	WP-C04
5	Account Management	6	4	2	0	14	11	WP-C05
6	Access Control Management	8	5	2	1	13	12	WP-C06
7	Continuous Vulnerability Management	7	4	3	0	13	13	WP-C07
8	Audit Log Management	12	3	8	1	18	14	WP-C08
9	Email and Web Browser Protections	7	2	4	1	11	15	WP-C09
10	Malware Defenses	7	3	4	0	14	16	WP-C10
11	Data Recovery	5	4	1	0	12	17	WP-C11
12	Network Infrastructure Management	8	1	6	1	15	18	WP-C12
13	Network Monitoring and Defense	11	0	6	5	14	19	WP-C13
14	Security Awareness and Skills Training	9	8	1	0	11	20	WP-C14
15	Service Provider Management	7	1	3	3	10	21	WP-C15
16	Application Software Security	14	0	11	3	18	22	WP-C16
17	Incident Response Management	9	3	5	1	12	23	WP-C17
18	Penetration Testing	5	0	3	2	9	24	WP-C18

APPENDIX C

IG1 Self-Assessment Checklist

A quick self-assessment of the 56 IG1 Safeguards, the essential cyber hygiene every enterprise should have. Answer each honestly; any "No" or "Partly" belongs on the gap analysis in Appendix E. For a scored assessment use the method in Chapter 30.

Control 1: Inventory and Control of Enterprise Assets

Table C-1. IG1 checklist, Control 1

Safeguard	Title (CIS wording)	In place?	Notes / evidence
1.1	“Establish and Maintain Detailed Enterprise Asset Inventory”	□ Yes □ Partly □ No	
1.2	“Address Unauthorized Assets”	□ Yes □ Partly □ No	

Control 2: Inventory and Control of Software Assets

Table C-2. IG1 checklist, Control 2

Safeguard	Title (CIS wording)	In place?	Notes / evidence
2.1	“Establish and Maintain a Software Inventory”	□ Yes □ Partly □ No	
2.2	“Ensure Authorized Software is Currently Supported”	□ Yes □ Partly □ No	
2.3	“Address Unauthorized Software”	□ Yes □ Partly □ No	

Control 3: Data Protection

Table C-3. IG1 checklist, Control 3

Safeguard	Title (CIS wording)	In place?	Notes / evidence
3.1	“Establish and Maintain a Data Management Process”	□ Yes □ Partly □ No	
3.2	“Establish and Maintain a Data Inventory”	□ Yes □ Partly □ No	
3.3	“Configure Data Access Control Lists”	□ Yes □ Partly □ No	
3.4	“Enforce Data Retention”	□ Yes □ Partly □ No	
3.5	“Securely Dispose of Data”	□ Yes □ Partly □ No	
3.6	“Encrypt Data on End-User Devices”	□ Yes □ Partly □ No	

Control 4: Secure Configuration of Enterprise Assets and Software

Table C-4. IG1 checklist, Control 4

Safeguard	Title (CIS wording)	In place?	Notes / evidence
4.1	“Establish and Maintain a Secure Configuration Process”	□ Yes □ Partly □ No	
4.2	“Establish and Maintain a Secure Configuration Process for Network Infrastructure”	□ Yes □ Partly □ No	
4.3	“Configure Automatic Session Locking on Enterprise Assets”	□ Yes □ Partly □ No	
4.4	“Implement and Manage a Firewall on Servers”	□ Yes □ Partly □ No	

Safeguard	Title (CIS wording)	In place?	Notes / evidence
4.5	“Implement and Manage a Firewall on End-User Devices”	□ Yes □ Partly □ No	
4.6	“Securely Manage Enterprise Assets and Software”	□ Yes □ Partly □ No	
4.7	“Manage Default Accounts on Enterprise Assets and Software”	□ Yes □ Partly □ No	

Control 5: Account Management

Table C-5. IG1 checklist, Control 5

Safeguard	Title (CIS wording)	In place?	Notes / evidence
5.1	“Establish and Maintain an Inventory of Accounts”	□ Yes □ Partly □ No	
5.2	“Use Unique Passwords”	□ Yes □ Partly □ No	
5.3	“Disable Dormant Accounts”	□ Yes □ Partly □ No	
5.4	“Restrict Administrator Privileges to Dedicated Administrator Accounts”	□ Yes □ Partly □ No	

Control 6: Access Control Management

Table C-6. IG1 checklist, Control 6

Safeguard	Title (CIS wording)	In place?	Notes / evidence
6.1	“Establish an Access Granting Process”	□ Yes □ Partly □ No	
6.2	“Establish an Access Revoking Process”	□ Yes □ Partly □ No	
6.3	“Require MFA for Externally-Exposed Applications”	□ Yes □ Partly □ No	
6.4	“Require MFA for Remote Network Access”	□ Yes □ Partly □ No	
6.5	“Require MFA for Administrative Access”	□ Yes □ Partly □ No	

Control 7: Continuous Vulnerability Management

Table C-7. IG1 checklist, Control 7

Safeguard	Title (CIS wording)	In place?	Notes / evidence
7.1	“Establish and Maintain a Vulnerability Management Process”	□ Yes □ Partly □ No	
7.2	“Establish and Maintain a Remediation Process”	□ Yes □ Partly □ No	
7.3	“Perform Automated Operating System Patch Management”	□ Yes □ Partly □ No	
7.4	“Perform Automated Application Patch Management”	□ Yes □ Partly □ No	

Control 8: Audit Log Management

Table C-8. IG1 checklist, Control 8

Safeguard	Title (CIS wording)	In place?	Notes / evidence
8.1	“Establish and Maintain an Audit Log Management Process”	□ Yes □ Partly □ No	
8.2	“Collect Audit Logs”	□ Yes □ Partly □ No	
8.3	“Ensure Adequate Audit Log Storage”	□ Yes □ Partly □ No	

Control 9: Email and Web Browser Protections

Table C-9. IG1 checklist, Control 9

Safeguard	Title (CIS wording)	In place?	Notes / evidence
9.1	“Ensure Use of Only Fully Supported Browsers and Email Clients”	□ Yes □ Partly □ No	
9.2	“Use DNS Filtering Services”	□ Yes □ Partly □ No	

Control 10: Malware Defenses

Table C-10. IG1 checklist, Control 10

Safeguard	Title (CIS wording)	In place?	Notes / evidence
10.1	“Deploy and Maintain Anti-Malware Software”	□ Yes □ Partly □ No	
10.2	“Configure Automatic Anti-Malware Signature Updates”	□ Yes □ Partly □ No	
10.3	“Disable Autorun and Autoplay for Removable Media”	□ Yes □ Partly □ No	

Control 11: Data Recovery

Table C-11. IG1 checklist, Control 11

Safeguard	Title (CIS wording)	In place?	Notes / evidence
11.1	“Establish and Maintain a Data Recovery Process”	□ Yes □ Partly □ No	
11.2	“Perform Automated Backups”	□ Yes □ Partly □ No	
11.3	“Protect Recovery Data”	□ Yes □ Partly □ No	
11.4	“Establish and Maintain an Isolated Instance of Recovery Data”	□ Yes □ Partly □ No	

Control 12: Network Infrastructure Management

Table C-12. IG1 checklist, Control 12

Safeguard	Title (CIS wording)	In place?	Notes / evidence
12.1	“Ensure Network Infrastructure is Up-to-Date”	□ Yes □ Partly □ No	

Control 14: Security Awareness and Skills Training

Table C-13. IG1 checklist, Control 14

Safeguard	Title (CIS wording)	In place?	Notes / evidence
14.1	“Establish and Maintain a Security Awareness Program”	□ Yes □ Partly □ No	
14.2	“Train Workforce Members to Recognize Social Engineering Attacks”	□ Yes □ Partly □ No	
14.3	“Train Workforce Members on Authentication Best Practices”	□ Yes □ Partly □ No	
14.4	“Train Workforce on Data Handling Best Practices”	□ Yes □ Partly □ No	
14.5	“Train Workforce Members on Causes of Unintentional Data Exposure”	□ Yes □ Partly □ No	
14.6	“Train Workforce Members on Recognizing and Reporting Security Incidents”	□ Yes □ Partly □ No	

Safeguard	Title (CIS wording)	In place?	Notes / evidence
14.7	“Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates”	□ Yes □ Partly □ No	
14.8	“Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks”	□ Yes □ Partly □ No	

Control 15: Service Provider Management

Table C-14. IG1 checklist, Control 15

Safeguard	Title (CIS wording)	In place?	Notes / evidence
15.1	“Establish and Maintain an Inventory of Service Providers”	□ Yes □ Partly □ No	

Control 17: Incident Response Management

Table C-15. IG1 checklist, Control 17

Safeguard	Title (CIS wording)	In place?	Notes / evidence
17.1	“Designate Personnel to Manage Incident Handling”	□ Yes □ Partly □ No	
17.2	“Establish and Maintain Contact Information for Reporting Security Incidents”	□ Yes □ Partly □ No	
17.3	“Establish and Maintain an Enterprise Process for Reporting Incidents”	□ Yes □ Partly □ No	

APPENDIX D

Implementation Status Worksheet

This worksheet records where the enterprise stands on every Safeguard of the CIS Controls v8.1. It lists Safeguards by ID only; the titles, asset types and security functions appear in Appendix A and in the Control chapters. The IG column shows the lowest Implementation Group in which CIS places each Safeguard. Because the Groups are cumulative, an enterprise working to IG2 records every IG1 and IG2 row and may mark IG3 rows as out of target scope.

D.1 How to complete the worksheet

- **Status:** use the evaluation scale from Chapter 6: Implemented (I), Partially implemented (P), Not implemented (N) or Not applicable (N/A). A Not applicable entry needs a written reason, for example "no on-premises wireless network".
- **Owner:** name a person or a role, not a team. Where an MSP operates the Safeguard, record the internal owner who oversees the provider.
- **Evidence ref:** cite the workpaper or document number (for example `WP-C05-03`) so a reviewer can find the record that supports the status.
- **Target date:** for any P or N row inside the target IG, the date by which the gap is to close. Carry these rows into the action plan in Appendix E.
- Date and initial the worksheet at each review. Re-assess at least annually and after any major change in the environment.

Table D-1. Worksheet header

Enterprise		**Target IG**	
Scope		**Assessment date**	
Completed by		**Reviewed by**	

Table D-2. Control 1: Inventory and Control of Enterprise Assets (5 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
1.1	IG1				
1.2	IG1				
1.3	IG2				
1.4	IG2				
1.5	IG3				

Table D-3. Control 2: Inventory and Control of Software Assets (7 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
2.1	IG1				
2.2	IG1				
2.3	IG1				
2.4	IG2				
2.5	IG2				
2.6	IG2				
2.7	IG3				

Table D-4. Control 3: Data Protection (14 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
3.1	IG1				
3.2	IG1				
3.3	IG1				
3.4	IG1				
3.5	IG1				
3.6	IG1				
3.7	IG2				
3.8	IG2				
3.9	IG2				
3.10	IG2				
3.11	IG2				
3.12	IG2				
3.13	IG3				
3.14	IG3				

Table D-5. Control 4: Secure Configuration of Enterprise Assets and Software (12 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
4.1	IG1				
4.2	IG1				
4.3	IG1				
4.4	IG1				
4.5	IG1				
4.6	IG1				
4.7	IG1				
4.8	IG2				
4.9	IG2				
4.10	IG2				
4.11	IG2				
4.12	IG3				

Table D-6. Control 5: Account Management (6 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
5.1	IG1				
5.2	IG1				
5.3	IG1				
5.4	IG1				
5.5	IG2				
5.6	IG2				

Table D-7. Control 6: Access Control Management (8 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
6.1	IG1				
6.2	IG1				
6.3	IG1				
6.4	IG1				
6.5	IG1				
6.6	IG2				
6.7	IG2				
6.8	IG3				

Table D-8. Control 7: Continuous Vulnerability Management (7 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
7.1	IG1				
7.2	IG1				
7.3	IG1				
7.4	IG1				
7.5	IG2				
7.6	IG2				
7.7	IG2				

Table D-9. Control 8: Audit Log Management (12 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
8.1	IG1				
8.2	IG1				
8.3	IG1				
8.4	IG2				
8.5	IG2				
8.6	IG2				
8.7	IG2				
8.8	IG2				
8.9	IG2				
8.10	IG2				
8.11	IG2				
8.12	IG3				

Table D-10. Control 9: Email and Web Browser Protections (7 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
9.1	IG1				
9.2	IG1				

Safeguard	IG	Status	Owner	Evidence ref	Target date
9.3	IG2				
9.4	IG2				
9.5	IG2				
9.6	IG2				
9.7	IG3				

Table D-11. Control 10: Malware Defenses (7 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
10.1	IG1				
10.2	IG1				
10.3	IG1				
10.4	IG2				
10.5	IG2				
10.6	IG2				
10.7	IG2				

Table D-12. Control 11: Data Recovery (5 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
11.1	IG1				
11.2	IG1				
11.3	IG1				
11.4	IG1				
11.5	IG2				

Table D-13. Control 12: Network Infrastructure Management (8 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
12.1	IG1				
12.2	IG2				
12.3	IG2				
12.4	IG2				
12.5	IG2				
12.6	IG2				
12.7	IG2				
12.8	IG3				

Table D-14. Control 13: Network Monitoring and Defense (11 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
13.1	IG2				
13.2	IG2				

Safeguard	IG	Status	Owner	Evidence ref	Target date
13.3	IG2				
13.4	IG2				
13.5	IG2				
13.6	IG2				
13.7	IG3				
13.8	IG3				
13.9	IG3				
13.10	IG3				
13.11	IG3				

Table D-15. Control 14: Security Awareness and Skills Training (9 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
14.1	IG1				
14.2	IG1				
14.3	IG1				
14.4	IG1				
14.5	IG1				
14.6	IG1				
14.7	IG1				
14.8	IG1				
14.9	IG2				

Table D-16. Control 15: Service Provider Management (7 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
15.1	IG1				
15.2	IG2				
15.3	IG2				
15.4	IG2				
15.5	IG3				
15.6	IG3				
15.7	IG3				

Table D-17. Control 16: Application Software Security (14 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
16.1	IG2				
16.2	IG2				
16.3	IG2				
16.4	IG2				
16.5	IG2				

Safeguard	IG	Status	Owner	Evidence ref	Target date
16.6	IG2				
16.7	IG2				
16.8	IG2				
16.9	IG2				
16.10	IG2				
16.11	IG2				
16.12	IG3				
16.13	IG3				
16.14	IG3				

Table D-18. Control 17: Incident Response Management (9 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
17.1	IG1				
17.2	IG1				
17.3	IG1				
17.4	IG2				
17.5	IG2				
17.6	IG2				
17.7	IG2				
17.8	IG2				
17.9	IG3				

Table D-19. Control 18: Penetration Testing (5 Safeguards)

Safeguard	IG	Status	Owner	Evidence ref	Target date
18.1	IG2				
18.2	IG2				
18.3	IG2				
18.4	IG3				
18.5	IG3				

Table D-20. Worksheet summary (count of Safeguards by status within the target IG)

Group	In scope	Implemented	Partially	Not implemented	N/A
IG1 (56)					
IG2 new (74)					
IG3 new (23)					
Total (153)					

Using the counts

A simple percentage of Safeguards implemented is a useful headline but hides weight: one missing backup Safeguard may matter more than three partial logging ones. Report the counts alongside the top gaps from Appendix E, not instead of them.

APPENDIX E

Gap Analysis and 12-Month Action Plan

This appendix turns the status recorded in Appendix D into a prioritised list of gaps and a dated plan to close them. It has three parts: guidance on how to rank gaps, a gap register, and a quarter-by-quarter action plan. The templates are deliberately plain so that they can be copied into a spreadsheet or a GRC tool without losing structure.

E.1 Guidance: from status to priorities

Step 1: fix the target

Agree the target Implementation Group with senior management before ranking anything (Chapter 3). A gap only exists against a target. A 40-person firm targeting IG1 does not carry a gap for an IG3 Safeguard such as passive asset discovery; recording it as one inflates the list and dilutes attention. Safeguards above the target IG can be listed separately as "future scope".

Step 2: list every P and N row inside the target

Copy each Partially implemented or Not implemented Safeguard from Appendix D into the gap register. Write the gap as a short Condition – Criteria – Effect statement: what was found, what the Safeguard expects, and what could go wrong as a result. "No restore has been tested in 14 months; recovery data should be tested regularly; ransomware recovery time is unknown" is far more useful than "backups weak".

Step 3: rate each gap

Use two simple ratings, each on a scale of 1 to 3:

- **Exposure (E):** how directly the gap enables a common attack against this enterprise. Missing MFA on internet-facing email, unpatched edge devices and untested backups usually rate 3. Gaps in documentation that affect no live control usually rate 1.
- **Effort (F):** 1 for a configuration change or a policy decision, 2 for a project of a few weeks with existing tools, 3 for work that needs new budget, new tooling or a change in how teams operate.

Priority = E × 2 – F, giving a range of –1 to 5. Treat 4–5 as "Quarter 1", 2–3 as "Quarters 2–3" and anything lower as "Quarter 4 or later". The formula is a starting point only; the CISO should adjust it where a regulator, customer contract or audit finding sets a firmer date.

Step 4: respect dependencies

Some Safeguards rest on others. Software allowlisting (2.5) is hard without a reliable software inventory (2.1, 2.4); vulnerability remediation (7.7) needs an asset inventory (1.1) to know what to scan; log reviews (8.11) need logs to be collected and centralised first (8.2, 8.9). When a high-priority gap depends on a lower one, move the prerequisite forward rather than starting the dependent work on sand.

Step 5: assign, date and fund

Every gap needs one named owner, a target quarter and an indication of cost (none, within budget, needs approval). Gaps that need approval go to the next management review with a short business case; the board reporting template in Appendix I shows how to present them.

> **India-specific dates**
>
> Where a gap touches an Indian obligation, for example log retention under the CERT-In Directions of April 2022, or reasonable security safeguards under the DPDP Act 2023 and Rules, note the instrument in the register and let legal or compliance confirm whether it sets a firmer timeline. Appendix G lists the usual touchpoints. Closing a CIS gap does not by itself establish compliance with any regulation.

E.2 Gap register

Table E-1. Gap register header

Enterprise		**Target IG**	
Based on worksheet dated		**Register version**	
Prepared by		**Approved by**	

Table E-2. Gap register (one row per Safeguard gap within the target IG)

Gap ID	Safeguard	Status (P/N)	Condition – Criteria – Effect	E (1–3)	F (1–3)	Priority	Depends on	Owner	Target quarter	Cost	Regulatory link
G-01											
G-02											
G-03											
G-04											
G-05											
G-06											
G-07											
G-08											
G-09											
G-10											

Table E-3. Worked example rows (fictional 600-employee Pune NBFC, target IG2)

Gap ID	Safeguard	Condition – Criteria – Effect	E	F	Priority	Target
G-01	6.4	Branch staff reach the loan system over VPN with password only; remote network access should need a second factor; one phished password gives an attacker an inside foothold.	3	1	5	Q1
G-02	11.5	Backups run nightly but no restore has been attempted since go-live; recovery should be proven by test; the NBFC cannot say how long a ransomware recovery would take.	3	2	4	Q1
G-03	8.9	Logs stay on each server for 30 days; logs should be gathered centrally and retained; evidence for an investigation, and for the CERT-In retention expectation, is lost.	2	2	2	Q2
G-04	15.4	Twelve of the 31 provider contracts have no security or breach-notice clause; contracts should carry security terms; the NBFC cannot enforce timely notice from a breached provider.	2	3	1	Q3 (renewal cycle)

E.3 12-month action plan

Group the register into four quarters. Each quarter should have a small number of themed outcomes rather than a long list of tasks, so that progress can be reported in a sentence. A typical pattern is: Quarter 1 closes the high-exposure, low-effort gaps (MFA, admin account separation, backup testing, edge patching); Quarter 2 builds the foundations that later work depends on (inventories, central logging, a vulnerability scanning cycle); Quarter 3 tackles contract, process and training gaps that follow business cycles; Quarter 4 consolidates, re-assesses and sets the next year's target.

Table E-4. 12-month action plan by quarter

Quarter	Outcome to be achieved	Gap IDs covered	Owner	Milestone / evidence of completion	Budget status	RAG at review
Q1 (months 1–3)						
Q1 (months 1–3)						
Q2 (months 4–6)						
Q2 (months 4–6)						
Q3 (months 7–9)						
Q3 (months 7–9)						
Q4 (months 10–12)						
Q4 (months 10–12)						

Table E-5. Quarterly progress review

Review date	Gaps closed this quarter	Gaps slipped (with reason)	New gaps raised	Decisions needed from management	Reviewed by

E.4 Closing a gap

A gap is closed only when the evidence shows the Safeguard operating, not when the project finishes. Before marking a row closed, re-run the relevant testing procedure from the Control chapter, file the result against the workpaper reference, and update Appendix D. For Safeguards with a stated frequency, such as monthly scanning or periodic restore tests, wait until at least one full cycle has run before recording Implemented; until then record Partially implemented with a note. Keep closed rows in the register for the year so that the annual re-assessment can see what moved.

> **Avoid the paper fix**
> Writing a policy closes a Govern-function gap such as 3.1 or 15.2 only if the policy is approved, communicated and followed. A new document with no operating evidence should stay at Partially implemented.

APPENDIX F

CIS Controls v8.1 to ISO/IEC 27001:2022 Crosswalk

Indicative Srida IT mapping

This crosswalk is Srida IT's own professional judgement. It is not the mapping published by the Center for Internet Security, and neither CIS nor ISO has reviewed or endorsed it. CIS publishes its own mappings of the Controls to other frameworks; where an official mapping is needed, for example to support an audit, use the current CIS mapping from cisecurity.org and reconcile any differences. Some rows and references are judgement calls that the reader should confirm.

F.1 How to read the crosswalk

ISO/IEC 27001:2022 has two layers. Clauses 4 to 10 set out the management system: context, leadership, planning, support, operation, performance evaluation and improvement. Annex A lists 93 reference controls in four themes: organisational (5.1–5.37), people (6.1–6.8), physical (7.1–7.14) and technological (8.1–8.34). The CIS Controls are prescriptive technical and operational Safeguards, so most of them land in Annex A; the Govern-function Safeguards and the review and exercise Safeguards also support the clauses.

Three cautions apply to every row:

- **The relationship is many-to-many and partial.** A CIS Safeguard often supports only part of an Annex A control, and the reverse. "Supports" is the right word; "satisfies" is not.
- **ISO is risk-based; CIS is prescriptive.** Under ISO/IEC 27001 the organisation selects controls through risk treatment (clause 6.1.3) and records them in a Statement of Applicability. Implementing the CIS Safeguards can be a sound way to implement selected Annex A controls, but it does not replace the risk assessment, the Statement of Applicability or the management system clauses.
- **Conformity is separate.** Implementing a Control does not establish ISO/IEC 27001 conformity, and ISO/IEC 27001 certification does not show that a CIS Implementation Group has been met.

Annex A control names below are short descriptive labels to help the reader; use the standard itself for the authoritative names and text.

F.2 Control-level crosswalk

Table F-1. CIS Controls v8.1 to ISO/IEC 27001:2022 Annex A and clauses (indicative Srida IT mapping)

CIS Control	Primary Annex A controls	Supporting Annex A controls	Clauses
1 Enterprise assets	5.9 Inventory of information and other associated assets	5.11 Return of assets; 8.1 User endpoint devices; 7.9 Assets off-premises	8.1
2 Software assets	5.9 Inventory of assets; 8.19 Installation of software on operational systems	5.32 Intellectual property rights (licensing); 8.7 Protection against malware (allowlisting)	8.1
3 Data protection	5.12 Classification; 5.33 Protection of records; 5.34 Privacy and protection of PII; 8.24 Use of cryptography	5.10 Acceptable use; 5.13 Labelling; 5.14 Information transfer; 7.10 Storage media; 7.14 Secure disposal or re-use; 8.3 Information access restriction; 8.10 Information deletion; 8.11 Data masking; 8.12 Data leakage prevention	6.1.2; 8.2
4 Secure configuration	8.9 Configuration management	8.1 User endpoint devices; 8.20 Networks security; 8.21 Security of network services; 7.7 Clear desk and clear screen (session lock); 6.7 Remote working (mobile workspaces)	8.1

CIS Control	Primary Annex A controls	Supporting Annex A controls	Clauses
5 Account management	5.16 Identity management; 5.18 Access rights	5.17 Authentication information; 8.2 Privileged access rights	8.1
6 Access control management	5.15 Access control; 5.18 Access rights; 8.5 Secure authentication	5.3 Segregation of duties (role design); 8.2 Privileged access rights; 8.3 Information access restriction; 6.5 Responsibilities after termination	8.1
7 Vulnerability management	8.8 Management of technical vulnerabilities	5.7 Threat intelligence; 8.32 Change management (patch deployment)	6.1.2; 8.1
8 Audit log management	8.15 Logging; 8.17 Clock synchronisation	8.16 Monitoring activities; 5.28 Collection of evidence; 5.22 Supplier service monitoring (provider logs)	8.1; 9.1
9 Email and browser protections	8.23 Web filtering; 8.7 Protection against malware	8.19 Installation of software (extensions); 5.14 Information transfer (email authentication such as DMARC); 8.21 Security of network services (DNS filtering)	8.1
10 Malware defences	8.7 Protection against malware	7.10 Storage media (removable media scanning); 8.1 User endpoint devices	8.1
11 Data recovery	8.13 Information backup	5.29 Information security during disruption; 5.30 ICT readiness for business continuity; 8.14 Redundancy	8.1
12 Network infrastructure management	8.20 Networks security; 8.22 Segregation of networks	8.21 Security of network services; 8.27 Secure system architecture and engineering principles; 8.9 Configuration management; 8.2 Privileged access rights (dedicated admin resources); 6.7 Remote working (VPN)	8.1
13 Network monitoring and defence	8.16 Monitoring activities; 8.20 Networks security	8.22 Segregation of networks (inter-segment filtering); 8.15 Logging (flow logs); 5.25 Assessment and decision on information security events	8.1; 9.1
14 Security awareness and skills training	6.3 Information security awareness, education and training	6.8 Information security event reporting; 5.10 Acceptable use	7.2 Competence; 7.3 Awareness
15 Service provider management	5.19 Information security in supplier relationships; 5.20 Addressing security within supplier agreements; 5.22 Monitoring, review and change management of supplier services	5.21 ICT supply chain; 5.23 Information security for use of cloud services; 5.11 Return of assets (decommissioning)	8.1 (externally provided processes)
16 Application software security	8.25 Secure development life cycle; 8.28 Secure coding; 8.29 Security testing in development and acceptance	8.4 Access to source code; 8.26 Application security requirements; 8.27 Secure architecture principles; 8.30 Outsourced development; 8.31 Separation of development, test and production; 8.33 Test information; 5.8 Security in project management	8.1
17 Incident response management	5.24 Incident management planning and preparation; 5.26 Response to information security incidents	5.5 Contact with authorities; 5.25 Assessment of events; 5.27 Learning from incidents; 5.28 Collection of evidence; 6.8 Event reporting	10.2 Nonconformity and corrective action
18 Penetration testing	8.8 Management of technical vulnerabilities	5.35 Independent review of information security; 8.29 Security testing; 8.34 Protection of systems during audit testing	9.1; 9.2

F.3 Key Safeguard-level links

The table below picks out Safeguards where the link to a specific Annex A control is direct enough to be useful during an ISO/IEC 27001 Statement of Applicability review or a combined audit. It is not exhaustive; Safeguards not listed take the control-level mapping above.

Table F-2. Selected CIS v8.1 Safeguards to ISO/IEC 27001:2022 Annex A (indicative Srida IT mapping)

Safeguard	Annex A	Note
1.1, 2.1	5.9	The CIS inventories give the technical detail that the ISO asset inventory expects.
2.2	8.8; 8.19	Unsupported software cannot receive fixes, so it is a vulnerability-management issue as much as an inventory one.
3.1	5.12; 5.33; 5.34	Data management process; also feeds clause 6.1.2 risk identification.
3.4, 3.5	5.33; 8.10; 7.14	Retention and disposal.
3.6, 3.9, 3.10, 3.11	8.24	Encryption on devices, removable media, in transit and at rest.
3.7	5.12; 5.13	Classification scheme and labelling.
3.13	8.12	Data loss prevention.
3.14	8.15	Logging access to sensitive data.
4.1, 4.2	8.9	Documented secure configuration baselines.
4.4, 4.5	8.20; 8.1	Host firewalls on servers and end-user devices.
4.7, 5.4	8.2; 5.17	Default and administrator accounts.
4.10, 4.11, 4.12	8.1; 6.7	Portable and mobile device controls.
5.2	5.17	Unique passwords as authentication information.
5.3, 6.2	5.18; 6.5	Removing dormant accounts and revoking access on exit or role change.
6.3, 6.4, 6.5	8.5	Multi-factor authentication for external, remote and administrative access.
6.8	5.15; 5.18; 5.3	Role-based access with periodic review.
7.3, 7.4, 7.7	8.8; 8.32	Patching and remediation.
7.5, 7.6	8.8	Internal and external vulnerability scanning.
8.4	8.17	Time synchronisation.
8.10	8.15; 5.33	Log retention; see also the CERT-In retention expectation in Appendix G.
8.11	8.16	Log review as a monitoring activity.
9.2, 9.3	8.23	DNS and URL filtering.
11.2, 11.3, 11.4, 11.5	8.13	Automated, protected, isolated and tested backups.
12.2, 13.4	8.22; 8.27	Network segmentation and filtering between segments.
13.1, 13.11	8.16; 5.25	Central alerting and tuning.
14.1–14.9	6.3; clause 7.3	Awareness programme and topic coverage.
14.6	6.8	Recognising and reporting incidents.
15.4	5.20	Security clauses in provider contracts.
15.5, 15.6	5.22	Provider assessment and monitoring.
16.4, 16.5	5.21; 8.28	Third-party software components.

Safeguard	Annex A	Note
16.8	8.31	Separation of production and non-production.
16.9	6.3; 8.28	Secure coding training for developers.
16.12, 16.13	8.29	Code-level checks and application penetration testing.
16.14	8.27; 8.26	Threat modelling within secure design.
17.2	5.5	Contacts for authorities and others; in India this includes CERT-In and any sector regulator.
17.4	5.24; 5.26	Documented incident response process.
17.7	5.24; 5.30	Exercising incident response.
17.8	5.27; clause 10.2	Post-incident review and corrective action.
18.1–18.5	8.8; 5.35	Penetration testing programme and remediation of findings.

F.4 Management system clauses the CIS Controls do not cover

Several ISO/IEC 27001 requirements have no real counterpart in the CIS Controls, even with the Govern function added in v8.1. An organisation using the CIS Controls as its control set and seeking ISO/IEC 27001 conformity must still build these:

- clause 4: context of the organisation, interested parties and the ISMS scope;
- clause 5: leadership commitment, the information security policy and assigned ISMS roles;
- clause 6.1.2 and 6.1.3: a defined risk assessment and risk treatment method, the Statement of Applicability and the risk treatment plan;
- clause 6.2: information security objectives and plans to achieve them;
- clause 7.5: control of documented information;
- clause 9.2 and 9.3: an internal audit programme and management review;
- clause 10: nonconformity handling and continual improvement of the ISMS as a whole.

The physical controls in Annex A (7.1–7.14) are also largely outside the CIS Controls, which assume physical security is handled elsewhere. Chapter 28 describes how to run CIS and ISO/IEC 27001 as one control set.

APPENDIX G

India Regulatory Touchpoints Matrix

Mapping is not compliance

This matrix shows where work done under a CIS Control is likely to produce evidence that is relevant to an Indian legal or regulatory obligation. It is a planning aid prepared by Srida IT, not legal advice. Implementing a Control does not establish compliance with any instrument listed here, and an instrument may demand more, or something different, than the Control. Every row should be confirmed against the current instrument: the instruments are described in general terms, they are amended and supplemented by circulars, FAQs and clarifications, and their applicability depends on the entity's sector, licence and size. Confirm the current text and your obligations with legal counsel or the compliance function before relying on any entry.

G.1 The instruments in brief

Table G-1. Indian instruments referred to in the matrix (general description only)

Short name	Instrument	Who it generally applies to	Themes relevant to the CIS Controls
CERT-In 2022	CERT-In Directions under section 70B(6) of the Information Technology Act, 2000, dated 28 April 2022, with later FAQs	Service providers, intermediaries, data centres, body corporates and government organisations, with specific duties for some categories such as VPN, cloud and data-centre providers	Reporting specified incidents to CERT-In within six hours of noticing them; keeping ICT system logs for a rolling 180 days within India; synchronising clocks to NTP servers of NIC or NPL, or traceable to them; naming a point of contact
SEBI CSCRF	SEBI Cybersecurity and Cyber Resilience Framework, issued by circular in August 2024, with later clarifications and phased timelines	SEBI-regulated entities, graded by category (for example market infrastructure institutions, qualified and mid-size entities)	Governance and policy, asset inventory, access and privilege controls, logging and monitoring including a security operations capability, vulnerability assessment and penetration testing, incident response, cyber resilience and audit
RBI	RBI directions on IT governance, risk, controls and assurance practices (Master Direction of November 2023) and earlier cyber security framework circulars for banks, with related directions for NBFCs, payment systems and co-operative banks	Banks, NBFCs above specified thresholds, payment system operators and other regulated entities, depending on the direction	Board-approved IT and information security governance, asset and configuration management, patch and vulnerability management, access controls, logging and a security operations centre for larger entities, business continuity, outsourcing oversight, incident reporting to RBI
IRDAI	IRDAI Information and Cyber Security Guidelines, 2023	Insurers, intermediaries and other IRDAI-regulated entities	Information security governance, risk assessment, asset management, access control, logging, vulnerability assessment and penetration testing, incident reporting, third-party risk and periodic audit
DPDP	Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025	Data Fiduciaries and Data Processors processing digital personal data in India, and some processing outside India connected to offering goods or services in India	Reasonable security safeguards to prevent personal data breach (Act s.8(5)); intimating breaches to the Data Protection Board and affected Data Principals (Act s.8(6)); the security measures and breach-intimation detail in the Rules (r.6 and r.7), such as encryption or similar measures, access control, logging and monitoring, backups and contractual safeguards with processors

CERT-In also empanels information security auditing organisations, and several sector regulators expect audits by such firms. That expectation is relevant to Control 18 and to the independent assessment described in Part IV.

G.2 Touchpoints matrix

Read each cell as "work under this Control is likely to support evidence for this theme of the instrument". A dash means there is no strong direct link; it does not mean the instrument is silent.

Table G-2. CIS Controls v8.1 against Indian regulatory themes (indicative; confirm each row against the current instrument)

CIS Control	CERT-In 2022	SEBI CSCRF	RBI	IRDAI	DPDP Act and Rules	Status
1 Enterprise assets	Knowing which systems must keep logs and feed incident reports	Asset inventory and criticality	Asset and configuration management	Asset management	Knowing where personal data is processed	
2 Software assets	–	Software inventory; unsupported software	Software inventory; end-of-life systems	Asset management	–	
3 Data protection	Incidents affecting data; data leaks as a reportable category	Data classification and protection	Data security, encryption, data leak prevention	Data classification and protection	Core link: reasonable safeguards, encryption or similar measures, retention and erasure, processor contracts	
4 Secure configuration	–	Secure configuration and hardening	Baseline configuration, hardening	System hardening	Part of reasonable security safeguards	
5 Account management	–	Identity and account management	User and privileged account management	Access management	Access control over personal data	
6 Access control	–	Access control, MFA, privileged access	Access control, MFA for critical systems	Access control	Access control over personal data (Rules)	
7 Vulnerability management	Exploited vulnerabilities as a reportable category	Vulnerability assessment and patching cadence	Patch and vulnerability management	Vulnerability assessment	Part of reasonable security safeguards	
8 Audit log management	Core link: 180-day log retention in India and NTP synchronisation	Logging, retention and monitoring	Logging and log review; SOC for larger entities	Logging and monitoring	Logs and monitoring to detect and investigate breaches; log retention in the Rules	
9 Email and browser	Phishing and malicious email as reportable categories	Email security	Email and internet security	Email security	–	
10 Malware defences	Malware and ransomware as reportable categories	Endpoint protection	Anti-malware, endpoint protection	Endpoint protection	Part of reasonable security safeguards	
11 Data recovery	–	Backup, recovery and cyber resilience	Backup, business continuity and recovery	Backup and business continuity	Backups to maintain continued processing in the event of compromise (Rules)	

CIS Control	CERT-In 2022	SEBI CSCRF	RBI	IRDAI	DPDP Act and Rules	Status
12 Network infrastructure	Clock source for network devices; logs from network devices	Network security and segmentation	Network security, secure remote access	Network security	–	
13 Network monitoring	Detecting incidents in time to meet the reporting window	Security operations and continuous monitoring	Security operations centre, monitoring	Monitoring	Detecting breaches to enable intimation	
14 Awareness and training	Staff knowing what to report and to whom	Awareness and training	Awareness programmes for staff and customers	Awareness and training	Staff handling of personal data	
15 Service providers	Provider logs and incident co-operation	Third-party and outsourcing risk	Outsourcing of IT services	Third-party and outsourcing risk	Contracts and safeguards with Data Processors	
16 Application security	Application compromise as a reportable category	Secure development and application testing	Secure SDLC, application security testing	Application security	Privacy and security in system design	
17 Incident response	Core link: six-hour reporting, point of contact	Incident response and reporting	Incident reporting to RBI and response plans	Incident reporting to IRDAI and CERT-In	Core link: breach intimation to the Board and Data Principals	
18 Penetration testing	Audits by CERT-In empanelled auditors where required	VAPT cadence and audit	Periodic VAPT and IS audit	VAPT and audit	Testing the effectiveness of safeguards	

G.3 Using the matrix

- **Start from the instrument, not the Control.** Legal or compliance should first confirm which instruments apply and what each one requires. Use the matrix afterwards to find the Controls whose evidence can be reused.
- **Watch for firmer requirements.** Indian instruments often fix numbers that the CIS Controls leave to the enterprise: reporting windows, log retention periods, audit frequencies and data-location rules. Where a regulator sets a number, it overrides the enterprise's own choice in the Control's process documents.
- **Record the link in the gap register.** When a gap in Appendix E touches an instrument, note the instrument so that its priority and target date reflect the regulatory exposure.
- **Re-check at each review.** Regulators issue new circulars and timelines often. Review this matrix at least annually and whenever a new direction is issued.

APPENDIX H

Completed Assessment Workpaper (Control 5)

This appendix shows what a finished workpaper looks like when the testing procedures in Chapter 11 (Control 5) are applied to a real-sized enterprise. The organisation, its people, systems, figures and findings are **entirely fictional** and are given only to illustrate the level of detail an assessor should record. The test IDs and procedures are exactly those of Control 5 in this manual (TP-C05-01 to TP-C05-14). A blank version of the workpaper can be built from the same columns.

> **How to read this sample.**
> Each test records what was looked at (the sample), what was found (the result on the four-point scale), where the evidence is filed (references of the form `E-C05-nn`) and the assessor's conclusion. Safeguard ratings are derived from the tests that relate to them, and the Control conclusion is derived from the Safeguard ratings. Implementation Groups describe scope, not maturity: the client chose IG2, so all six Safeguards of Control 5 are in scope.

H.1 Engagement details

Table H-1. WP-C05 header

Field	Entry
Workpaper	WP-C05 Control 5: Account Management
Client (fictional)	A 450-employee Coimbatore textile exporter with a spinning mill, two weaving units, a dyeing unit and a head office; referred to below as “the Exporter”
Implementation Group in scope	IG2 (Safeguards 5.1 to 5.6)
Review period	1 October 2025 to 30 September 2026 (four quarters)
Fieldwork dates	12 to 23 October 2026
In-scope systems	Directory and cloud productivity suite (identity provider); ERP (finance, purchase, sales, inventory); payroll SaaS; export documentation portal (vendor-hosted); mill production reporting application; firewall and core switches; 380 Windows endpoints; 14 servers
Client contacts	Head of IT (owner of Control 5); HR Manager; ERP application owner; IT administrator (two); external MSP account manager
Prepared by / date	Assessor A, 23 October 2026
Reviewed by / date	Engagement reviewer B, 28 October 2026
Evaluation scale	Implemented / Partially implemented / Not implemented / Not applicable

H.2 Populations and data sources

Whole-population analysis was used wherever the data could be extracted. Each population was extracted by the client's IT administrator in the assessor's presence, and completeness was checked by comparing record counts with the system's own on-screen totals.

Table H-2. Populations used in testing

Population	Source and extraction date	Count	Completeness check	Ref
Enabled directory accounts	Identity provider export, 13 Oct 2026	512	Matched admin console total	E-C05-01
Enabled ERP accounts	ERP user master report, 13 Oct 2026	236	Matched licence count screen	E-C05-02

Enabled export portal accounts	Vendor-supplied user list, 14 Oct 2026	41	Confirmed by vendor e-mail	E-C05-03
Enabled mill production app accounts	Database query of user table, 14 Oct 2026	58	Query re-run by assessor	E-C05-04
Current workers	HR master (employees) and contractor register, 13 Oct 2026	451 employees, 37 contractors	Agreed to September payroll headcount	E-C05-05
Leavers and movers in period	HR exit and transfer reports, 1 Oct 2025 to 30 Sep 2026	68 leavers, 22 movers	Agreed to payroll full-and-final settlements	E-C05-06
Privileged group members	Directory, cloud suite and ERP admin role exports, 13 Oct 2026	19	Compared across three exports	E-C05-07
Service accounts (discovered)	Directory filter, database logins, cloud app registrations, 15 Oct 2026	44	Compared with client inventory	E-C05-08

H.3 Test results

Safeguard 5.1: account inventory and quarterly validation

Table H-3. WP-C05 tests TP-C05-01 to TP-C05-03 and TP-C05-14

Test ID	Method and procedure (summary)	Sample	Result	Evidence	Conclusion
TP-C05-01	Examine the account management standard and the inventory for coverage of user, administrator and service accounts and the minimum fields	Standard v2.1 (approved March 2026); inventory workbook covering directory, ERP, payroll SaaS and export portal	Partially implemented	E-C05-09 standard; E-C05-10 inventory	Inventory holds name, username, department, start and end dates for human accounts. The mill production application (58 accounts) is missing from the inventory although it is in the software inventory. Service accounts are listed only by username.
TP-C05-02	Re-perform reconciliation of active accounts in the directory and two or more critical applications to HR and contractor records	All 512 directory, 236 ERP and 58 mill application accounts, against 488 current workers, as at 13 Oct 2026	Partially implemented	E-C05-11 reconciliation workpaper	Directory: 6 enabled accounts with no current worker (all leavers from August and September 2026). ERP: 2 unmatched. Mill application: 14 unmatched, including 9 shift-supervisor IDs shared across shifts. All 22 referred to the client; 13 disabled during fieldwork (E-C05-12).
TP-C05-03	Inspect quarterly validation records for each quarter of the period	Quarters ending Dec 2025, Mar 2026, Jun 2026, Sep 2026	Partially implemented	E-C05-13 validation packs	Validations for December, March and September were signed by the Head of IT with actions evidenced. The June quarter was not performed (staff vacancy). Validations cover the directory and ERP only.
TP-C05-14	Interview IAM administrator, HR and two line managers on how validation is done and how contractor end dates are captured	IT administrator; HR Manager; Weaving Unit 1 manager; Accounts manager	Partially implemented	E-C05-14 interview notes	Managers confirm they receive the list and reply by e-mail, but one manager had approved without checking. Contractor end dates are captured by HR for agency staff but not for machine-vendor technicians, who are added directly by IT.

Safeguard 5.2: unique passwords

Table H-4. WP-C05 tests TP-C05-04 and TP-C05-05

Test ID	Method and procedure (summary)	Sample	Result	Evidence	Conclusion

TP-C05-04	Inspect password settings in the directory, email tenant, applications and network devices against the 8-character (with MFA) and 14-character (without MFA) minimums and breached-password screening	Identity provider policy; ERP; payroll SaaS; export portal; mill application; firewall; 2 core switches	Partially implemented	E-C05-15 configuration screenshots	Identity provider: 12 characters, MFA enforced, breached-password screening on: meets the rule. ERP (no MFA): 8 characters, below the 14-character minimum for accounts without MFA. Mill application: no length rule. Network devices: 16-character unique admin passwords held in vault.
TP-C05-05	Sample endpoints and servers for unique local administrator credentials; check network devices and appliances for shared or default passwords	20 endpoints across four sites; 6 servers; firewall, 2 switches, 2 printers, 1 CCTV recorder	Implemented	E-C05-16 local admin tool report; E-C05-17 vault entries	All 20 endpoints and 6 servers are enrolled in the local administrator password tool with unique, 30-day rotated passwords. Coverage report shows 377 of 380 endpoints enrolled; the 3 others are spare stock not in use. Appliance credentials unique and vaulted.

Safeguard 5.3: dormant accounts

Table H-5. WP-C05 tests TP-C05-06 and TP-C05-07

Test ID	Method and procedure (summary)	Sample	Result	Evidence	Conclusion
TP-C05-06	Re-perform last sign-in analysis to find enabled accounts inactive for more than 45 days; inspect the automation and its run history	All enabled accounts in directory (512) and ERP (236); weekly job history for 52 weeks	Partially implemented	E-C05-18 sign-in analysis; E-C05-19 job log	Directory: weekly job ran 50 of 52 weeks and disables accounts at 45 days; 2 enabled dormant accounts, both on the exception list. ERP: no dormancy control; 17 enabled accounts inactive for over 45 days, 11 of them over 120 days.
TP-C05-07	Examine the dormant-account exception list for owner, justification and quarterly review	Full list (4 entries)	Implemented	E-C05-20 exception list	Four entries (two break-glass admin accounts, two statutory audit accounts), each with an owner, justification and review dated within the last quarter.

Safeguard 5.4: dedicated administrator accounts

Table H-6. WP-C05 tests TP-C05-08 and TP-C05-09

Test ID	Method and procedure (summary)	Sample	Result	Evidence	Conclusion
TP-C05-08	Inspect privileged group and role membership to confirm only dedicated admin accounts hold privileges, each mapped to a named person	All 19 privileged members across directory, cloud suite and ERP	Partially implemented	E-C05-07 exports; E-C05-21 mapping	17 of 19 are dedicated `adm-` accounts mapped to named people (including 3 MSP engineers). 2 exceptions: the Finance Controller's everyday account holds ERP super-user rights, and a former MSP engineer's admin account remained enabled (disabled during fieldwork, E-C05-12).
TP-C05-09	Re-perform or inspect attempts to use admin accounts for email and browsing; inspect local administrators group on endpoints	5 admin accounts; 20 endpoints from TP-C05-05	Implemented	E-C05-22 test screenshots; E-C05-23 local group report	Admin accounts have no mailbox licence and conditional access blocks browser sign-in outside the jump host. No everyday user account is in the local administrators group on any sampled endpoint.

Safeguard 5.5: service account inventory

Table H-7. WP-C05 tests TP-C05-10 and TP-C05-11

Test ID	Method and procedure (summary)	Sample	Result	Evidence	Conclusion
TP-C05-10	Examine the service account inventory for department owner, purpose and review date, and compare with discovered service accounts	Client inventory (29 entries) against 44 discovered	Not implemented	E-C05-08 discovery; E-C05-24 inventory	The client list records username and system only; no owner, purpose or review date. 15 discovered service accounts are absent, including 4 database logins used by the mill application and 3 cloud app registrations with mail-read permission.
TP-C05-11	Inspect quarterly service account reviews and sample accounts for owner confirmation, disablement and credential handling	Four quarters; 10 service accounts	Not implemented	E-C05-25 IT administrator statement	No service account review was performed in the period. Of 10 sampled accounts, 3 have passwords vaulted; 7 have passwords unchanged since 2022 or earlier and set never to expire.

Safeguard 5.6: central account management

Table H-8. WP-C05 tests TP-C05-12 and TP-C05-13

Test ID	Method and procedure (summary)	Sample	Result	Evidence	Conclusion
TP-C05-12	Examine identity architecture and application register for the authoritative source, integration coverage and recorded exceptions	Application register (11 in-scope applications)	Partially implemented	E-C05-26 architecture; E-C05-27 register	The identity provider is the authoritative source and is fed by payroll HR events. 7 of 11 applications are federated (64%). ERP and mill application are not integrated and are not on an exception register; export portal and one SaaS are recorded as exceptions with monthly vendor reconciliation.
TP-C05-13	Trace a sample of leavers and movers through the directory and connected applications	20 leavers (weighted to 6 involuntary and 4 with privileged access) and 5 movers	Partially implemented	E-C05-28 trace sheet	All 25 directory changes were driven by HR events within one working day, and federated applications followed automatically. In the ERP, 3 of 20 leavers were disabled 9 to 34 days late through manual e-mail requests; 1 of 5 movers kept prior-role ERP access.

H.4 Safeguard ratings

Table H-9. WP-C05 Safeguard evaluation summary

Safeguard	IG	Tests	Rating	Basis
5.1	IG1	TP-C05-01, 02, 03, 14	Partially implemented	Inventory and validations exist but omit one application, missed a quarter and found unmatched accounts
5.2	IG1	TP-C05-04, 05	Partially implemented	Strong in the directory and endpoints; ERP and mill application fall below the length rule
5.3	IG1	TP-C05-06, 07	Partially implemented	Automated in the directory; absent in the ERP
5.4	IG1	TP-C05-08, 09	Partially implemented	Largely in place; one everyday account holds ERP super-user rights
5.5	IG2	TP-C05-10, 11	Not implemented	No inventory with required fields and no reviews
5.6	IG2	TP-C05-12, 13	Partially implemented	Central service in place for 64% of applications; ERP and mill application outside it

H.5 Findings

Findings are written as Condition, Criteria, Cause, Effect and Recommendation, and are rated High, Medium or Low on the assessor's judgement of likelihood and impact. Management responses were obtained on 27 October 2026.

Table H-10. WP-C05 findings register

Ref	Safeguard	Rating	Finding	Recommendation	Management response and target date
F-C05-01	5.5	High	**Condition:** No service account inventory with owner, purpose and review date; 15 undiscovered accounts; 7 of 10 sampled with non-expiring passwords set years ago; no quarterly review. **Criteria:** 5.5. **Cause:** Service accounts created by vendors at installation and never handed over. **Effect:** Over-privileged, unmonitored credentials, including mail-read app registrations, available for misuse.	Build the inventory with owners from IT and each business function; vault or rotate all credentials; disable unclaimed accounts after 14 days' notice; start quarterly reviews.	Agreed. Inventory by 30 Nov 2026; first review by 31 Dec 2026. Owner: Head of IT.
F-C05-02	5.1, 5.3, 5.6	High	**Condition:** ERP and mill application are outside central account management; 17 dormant ERP accounts; 3 leavers removed late; 9 shared supervisor IDs. **Criteria:** 5.1, 5.3, 5.6. **Cause:** Legacy applications without federation support; reliance on e-mail requests. **Effect:** Former staff and unattributable users can reach financial and production data.	Federate the ERP (vendor confirms support in the current release with vendor); until then run a weekly dormancy and leaver reconciliation. Replace shared supervisor IDs with named accounts.	Agreed. Weekly reconciliation from 1 Nov 2026; federation by 31 Mar 2027; named IDs by 31 Dec 2026. Owner: ERP application owner.
F-C05-03	5.1	Medium	**Condition:** June 2026 quarterly validation not performed; validations exclude two applications; a manager approved without checking. **Criteria:** 5.1 (at least quarterly). **Cause:** Single-person dependency; no reviewer guidance. **Effect:** Unauthorised accounts can persist between validations.	Assign a deputy, add all applications to the validation pack, and give managers a short checklist with escalation for late returns.	Agreed. Effective from the December 2026 quarter. Owner: Head of IT.
F-C05-04	5.2	Medium	**Condition:** ERP minimum password length is 8 without MFA; mill application has no length rule. **Criteria:** 5.2. **Cause:** Application defaults never changed. **Effect:** Passwords vulnerable to guessing.	Set 14 characters in the ERP until it is federated with MFA; apply a length rule or a front-end login control to the mill application.	Agreed. By 30 Nov 2026. Owner: ERP application owner.
F-C05-05	5.4	Medium	**Condition:** Finance Controller's everyday account holds ERP super-user rights; a former MSP engineer's admin account was still enabled. **Criteria:** 5.4. **Cause:** Convenience; MSP staff changes not notified. **Effect:** Privileged ERP access exposed to phishing; former third-party access to systems.	Issue a dedicated ERP admin account with approval workflow; require the MSP to notify staff changes within one working day under the contract.	Agreed. Former MSP account disabled 16 Oct 2026; ERP admin account by 15 Nov 2026. Owner: Head of IT.

H.6 Overall Control conclusion

Table H-11. WP-C05 Control 5 conclusion

Item	Conclusion

IG1 Safeguards (5.1 to 5.4)	All four Partially implemented. The foundations are sound: the directory is fed by HR, the local administrator password tool covers the endpoint estate, administrator accounts are largely separated and blocked from mail, and the directory dormancy job runs reliably. The weaknesses lie in the two applications outside central management and in one missed quarterly validation.
IG2 Safeguards (5.5, 5.6)	5.5 Not implemented; 5.6 Partially implemented.
Overall Control 5 rating	**Partially implemented.** The Exporter does not yet meet IG2 for Control 5 and does not fully meet IG1. The most significant risk is unmanaged service accounts (F-C05-01) and the ERP and mill application sitting outside the account lifecycle (F-C05-02).
Srida IT maturity indicator (separate from IG)	Defined, moving towards Managed in the directory scope.
Dependencies noted for other workpapers	WP-C06: MFA is absent on the ERP, so 6.3 and 6.5 testing should cover it. WP-C04: default account handling on the mill application database (4.7). WP-C15: MSP staff-change notification.
Follow-up	Re-test F-C05-01 and F-C05-02 in February 2027; full re-assessment of Control 5 in the next annual cycle.
Limitations	The export portal user list was supplied by the vendor and could not be extracted independently; reliance was placed on the vendor's e-mail confirmation. Testing does not certify the Exporter against any standard; CIS does not operate a certification scheme for organisations.

H.7 Sign-off

Table H-12. WP-C05 sign-off

Role	Name	Date
Prepared by (assessor)	Assessor A	23 October 2026
Reviewed by (engagement reviewer)	Engagement reviewer B	28 October 2026
Acknowledged by (client Head of IT)	Head of IT, the Exporter	29 October 2026

APPENDIX I

Board Reporting Template

Boards and audit committees do not need Safeguard-level detail. They need to know whether the enterprise is protected to the level it chose, where it is not, what that means for the business and what decision is being asked of them. This template fits on two pages and is meant for a quarterly or half-yearly report. Fill it from Appendices D and E; do not create new numbers for the board that the working documents cannot support.

I.1 Writing guidance

- **Lead with the answer.** The first section should say, in two or three sentences, whether the position has improved, held or worsened since the last report, and why.
- **Use business language.** Write "a stolen staff password would let an attacker into the branch network" rather than "6.4 not implemented". Put Safeguard IDs in brackets for traceability only.
- **Show trend, not just status.** A single percentage means little; the same figure shown against the last three reports tells the board whether the programme is working.
- **Separate IG progress from maturity.** Implementation Group coverage shows which Safeguards are in place. The Srida IT maturity indicators (initial, defined, managed, optimised) describe how well they are run. Report them as two different things.
- **Ask for decisions explicitly.** If the board must approve budget, accept a risk or set a target, say so in the decisions section, with the options and their consequences.
- **Do not overstate.** Never describe the enterprise as certified against the CIS Controls or as "fully compliant". There is no organisational certification for the CIS Controls, and coverage of Safeguards does not by itself establish compliance with any Indian regulation.

I.2 Template

Table I-1. Report header

Enterprise		**Reporting period**	
Presented to		**Date of meeting**	
Presented by (CISO or equivalent)		**Classification**	
Target Implementation Group		**Date target was approved**	

1. Summary position

Table I-2. Summary position (two to three sentences each)

Overall direction since last report (improved / held / worsened)	
Main reason	
Most significant open exposure	
Decision required from the board	

2. Coverage of the target Implementation Group

Table I-3. Safeguard coverage trend (from Appendix D)

Group	In scope	Implemented (this period)	Partially	Not implemented	Implemented (previous period)	Implemented (two periods ago)
IG1						

Group	In scope	Implemented (this period)	Partially	Not implemented	Implemented (previous period)	Implemented (two periods ago)
IG2 (new Safeguards)						
IG3 (new Safeguards)						

3. Control heat map

Give each of the 18 Controls a single rating: Green (all in-scope Safeguards implemented), Amber (some partially implemented, plan on track) or Red (key Safeguards not implemented or plan slipped). Add a one-line reason for every Amber and Red.

Table I-4. Control status by RAG rating

Control	RAG	Reason (Amber or Red only)	Control	RAG	Reason (Amber or Red only)
1			10		
2			11		
3			12		
4			13		
5			14		
6			15		
7			16		
8			17		
9			18		

4. Top risks from open gaps

Table I-5. Top five open gaps in business terms (from Appendix E)

#	What could happen	Safeguards (for reference)	Current mitigation	Fix and target date	Owner
1					
2					
3					
4					
5					

5. Key indicators

Table I-6. Operational indicators (choose five to eight and keep them stable between reports)

Indicator	Target	This period	Previous period	Comment
Accounts with MFA where required (6.3–6.5), %				
Critical vulnerabilities open beyond the agreed fix time (7.7)				
Last successful restore test and recovery time achieved (11.5)				
Assets in inventory with up-to-date endpoint protection (1.1, 10.1), %				
Staff completing awareness training (14.1), %				
Critical service providers assessed in the last 12 months (15.5), %				

Indicator	Target	This period	Previous period	Comment
Incidents reported to regulators or CERT-In within the required window				

6. Incidents and external events

Table I-7. Significant incidents, regulatory notifications and audit findings this period

Date	Event	Impact	Notified to (regulator, CERT-In, customers)	Lessons and actions

7. Regulatory and assurance status

Table I-8. Regulatory and assurance commitments (see Appendix G)

Obligation or assurance activity	Next due date	Status	Comment

8. Decisions requested

Table I-9. Decisions requested from the board

#	Decision	Options considered	Recommendation	Cost or risk if not approved	Board decision
1					
2					
3					

> **For a small firm**
>
> A 40-person firm working to IG1 can shrink this to one page: the summary position, the IG1 coverage row, the top three gaps and any decision needed. Present it to the partners or owners twice a year and minute the decisions.

APPENDIX J

References

The references below were used in preparing this manual or are recommended for further reading. Items should be checked against the issuing body's current publication before reliance; titles, dates, version numbers and web addresses change. The listing of a resource does not imply any affiliation with, or endorsement by, its publisher.

J.1 CIS Critical Security Controls

- Center for Internet Security. *CIS Critical Security Controls Version 8.1*. June 2024 (guide document dated August 2024). Available at `https://www.cisecurity.org/controls/v8-1`.
- Licence: the CIS Controls are made available under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License (CC BY-NC-ND 4.0), `https://creativecommons.org/licenses/by-nc-nd/4.0/`. This manual reproduces only the Control and Safeguard titles and their CIS attributes (asset type, security function and Implementation Group); all other text is Srida IT's own. It is distributed free and non-commercially. Commercial use of the CIS Controls requires CIS's permission; see the terms published by CIS.
- Center for Internet Security. *CIS Controls Implementation Groups* guidance and the Implementation Group descriptions within the v8.1 guide.
- Center for Internet Security. *CIS Community Defense Model* (CDM), v3.0, September 2026.
- Center for Internet Security. *CIS Controls Self Assessment Tool* (CSAT) for current availability and editions.
- Center for Internet Security. *CIS Benchmarks*: consensus secure configuration guides for operating systems, cloud platforms, network devices and applications.
- Center for Internet Security. *CIS Controls Navigator* and the CIS mappings of the Controls to other frameworks, including ISO/IEC 27001 and NIST CSF 2.0.
- Center for Internet Security. CIS Controls companion guides, for example for cloud, mobile and small enterprises for current titles.

J.2 International standards and frameworks

- ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, with Amendment 1:2024 (climate action changes).
- ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection — Information security controls*.
- ISO/IEC 27005:2022. *Guidance on managing information security risks*.
- ISO/IEC 27701:2025. Privacy information management systems for edition and title.
- National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, 26 February 2024.
- National Institute of Standards and Technology. SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, with later updates.
- National Institute of Standards and Technology. SP 800-61, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, Revision 3, April 2025.
- National Institute of Standards and Technology. SP 800-115, *Technical Guide to Information Security Testing and Assessment*, 2008.
- PCI Security Standards Council. *PCI DSS v4.0.1*, June 2024, for format comparison with the Requirements and Testing Procedures style.

J.3 Indian legal and regulatory instruments

- Information Technology Act, 2000, as amended, in particular section 70B (Indian Computer Emergency Response Team) and section 43A for the status of section 43A after the DPDP Act.

- CERT-In. Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In, 28 April 2022, and the associated FAQs.
- CERT-In. Guidelines and empanelment of information security auditing organisations for the current list and any audit guidelines issued.
- Securities and Exchange Board of India. *Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities*, circular dated 20 August 2024, and subsequent clarifications and timeline extensions.
- Reserve Bank of India. *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices*, 7 November 2023.
- Reserve Bank of India. *Cyber Security Framework in Banks*, circular of 2 June 2016, and related cyber security directions for urban co-operative banks, NBFCs and payment system operators.
- Reserve Bank of India. *Master Direction on Digital Payment Security Controls*, 2021.
- Reserve Bank of India. Directions on outsourcing of information technology services, 2023.
- Insurance Regulatory and Development Authority of India. *Information and Cyber Security Guidelines, 2023*.
- Digital Personal Data Protection Act, 2023 (No. 22 of 2023), in particular sections 8(5) and 8(6).
- Digital Personal Data Protection Rules, 2025, in particular rules 6 (reasonable security safeguards) and 7 (intimation of personal data breach) for the notified text and commencement dates.

J.4 Open-source tools named as examples

The manual names a small number of open-source projects as examples of tool categories. They are named for illustration only; their suitability, licence terms and support status must be assessed by the enterprise.

- osquery (endpoint inventory and query).
- Wazuh (host-based detection and log analysis).
- OpenVAS / Greenbone Community Edition (vulnerability scanning).
- Velociraptor (endpoint visibility and digital forensics).

J.5 Srida IT companion publications

- Srida IT. *NIST Cybersecurity Framework 2.0 Requirements and Testing Procedures, with an India Lens*, v1.0, November 2026.
- Srida IT. *ISO/IEC 27001:2022 Requirements and Testing Procedures*, v1.0.
- Srida IT. *Digital Personal Data Protection Act and Rules Requirements and Testing Procedures*, v1.1.



Building Digital Trust

SRIDA-CIS-RTP-001 · Version 1.0

© 2026 Srida IT · CC BY-NC-ND 4.0 · sridait.com · info@sridait.com

Free edition · Independent professional guidance. Not a CIS publication.
CIS Controls © Center for Internet Security, CC BY-NC-ND 4.0.