SRIDA IT PROFESSIONAL REFERENCE PUBLICATION

ISO/IEC 27001:2022

Information Security Management System (ISMS)

Requirements, Implementation Guidance & Audit Testing Procedures

DOCUMENT ID
SRIDA-ISMS-27001-RTP-001

VERSION
1.0

STATUS
Final — Approved for Publication

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

Independent professional guidance.
Not an official ISO or IEC publication.



ISO/IEC 27001:2022 — Information Security Management System (ISMS)

Requirements, Implementation Guidance & Audit Testing Procedures

Prepared by

Rajendra Bodda

Chief Information Security Officer (CISO)

SAMPLE

Published by Srida IT

SRIDA-ISMS-27001-RTP-001 · Version 1.0 · October 2026

This publication is an independently developed professional guidance document prepared by Srida IT. It is not an official ISO or IEC publication, does not replace the licensed ISO/IEC 27001:2022 or ISO/IEC 27002:2022 standards, and does not confer certification or accreditation.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT

Document Information and Control

Field	Value
Document title	ISO/IEC 27001:2022 — Information Security Management System (ISMS)
Subtitle	Requirements, Implementation Guidance & Audit Testing Procedures
Document identifier	SRIDA-ISMS-27001-RTP-001
Version	1.0
Status	Final — Approved for Publication
Classification	Srida IT Professional Reference Publication
Author	Rajendra Bodda, Chief Information Security Officer (CISO)
Publisher	Srida IT
Publication year	2026
Issue date	October 2026
Reference standards	ISO/IEC 27001:2022 (incl. Amd 1:2024); ISO/IEC 27002:2022
Next review	Annually, or on revision of the referenced standards

Version history

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

Approval

Role	Name	Date
Approved for publication	Rajendra Bodda, Chief Information Security Officer (CISO)	25 October 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.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT

Table of Contents

Part I Foundations 17

Chapter 1 Introduction to ISO/IEC 27001:2022 18
Chapter 2 ISO 27001 Structure and Certification Overview 23
Chapter 3 Information Security Management System Principles 27
Chapter 4 ISO/IEC 27001, ISO/IEC 27002 and Related Standards 31
Chapter 5 Terminology, Definitions and Abbreviations 35
Chapter 6 How to Use This Requirements and Testing Manual 39
Chapter 7 Audit Methodology, Evidence and Sampling Principles 44

Part II ISMS Requirements (Clauses 4–10) 49

Chapter 8 Clause 4 — Context of the organization 50
Clause 4.1 Understanding the organization and its context 51
Clause 4.2 Understanding the needs and expectations of interested parties 56
Clause 4.3 Determining the scope of the information security management system 60
Clause 4.4 Information security management system 64
Chapter 9 Clause 5 — Leadership 68
Clause 5.1 Leadership and commitment 69
Clause 5.2 Policy 73
Clause 5.3 Organizational roles, responsibilities and authorities 77
Chapter 10 Clause 6 — Planning 81
Clause 6.1.1 Actions to address risks and opportunities: General 82
Clause 6.1.2 Information security risk assessment 86
Clause 6.1.3 Information security risk treatment 91
Clause 6.2 Information security objectives and planning to achieve them 96
Clause 6.3 Planning of changes 100
Chapter 11 Clause 7 — Support 105
Clause 7.1 Resources 106
Clause 7.2 Competence 111
Clause 7.3 Awareness 116
Clause 7.4 Communication 120
Clause 7.5 Documented information (7.5.1 General, 7.5.2 Creating and updating, 7.5.3 Control of documented information) 125
Chapter 12 Clause 8 — Operation 130
Clause 8.1 Operational planning and control 131
Clause 8.2 Information security risk assessment 136
Clause 8.3 Information security risk treatment 140
Chapter 13 Clause 9 — Performance evaluation 144
Clause 9.1 Monitoring, measurement, analysis and evaluation 145
Clause 9.2 Internal audit (9.2.1 General, 9.2.2 Internal audit programme) 149
Clause 9.3 Management review (9.3.1 General, 9.3.2 Management review inputs, 9.3.3 Management review results) 153
Chapter 14 Clause 10 — Improvement 157
Clause 10.1 Continual improvement 158
Clause 10.2 Nonconformity and corrective action 162

Part III Annex A Information Security Controls 167

Chapter 15 A.5 Organizational controls 168
A.5.1 Policies for information security 170
A.5.2 Information security roles and responsibilities 175
A.5.3 Segregation of duties 179
A.5.4 Management responsibilities 183
A.5.5 Contact with authorities 187

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT

A.5.6 Contact with special interest groups 191
A.5.7 Threat intelligence 195
A.5.8 Information security in project management 200
A.5.9 Inventory of information and other associated assets 204
A.5.10 Acceptable use of information and other associated assets 208
A.5.11 Return of assets 212
A.5.12 Classification of information 216
A.5.13 Labelling of information 220
A.5.14 Information transfer 224
A.5.15 Access control 228
A.5.16 Identity management 232
A.5.17 Authentication information 236
A.5.18 Access rights 240
A.5.19 Information security in supplier relationships 244
A.5.20 Addressing information security within supplier agreements 248
A.5.21 Managing information security in the ICT supply chain 252
A.5.22 Monitoring, review and change management of supplier services 256
A.5.23 Information security for use of cloud services 260
A.5.24 Information security incident management planning and preparation 264
A.5.25 Assessment and decision on information security events 268
A.5.26 Response to information security incidents 272
A.5.27 Learning from information security incidents 277
A.5.28 Collection of evidence 281
A.5.29 Information security during disruption 285
A.5.30 ICT readiness for business continuity 289
A.5.31 Legal, statutory, regulatory and contractual requirements 293
A.5.32 Intellectual property rights 297
A.5.33 Protection of records 301
A.5.34 Privacy and protection of PII 305
A.5.35 Independent review of information security 309
A.5.36 Compliance with policies, rules and standards for information security 313
A.5.37 Documented operating procedures 317

Chapter 16 **A.6 People controls** 321
A.6.1 Screening 322
A.6.2 Terms and conditions of employment 327
A.6.3 Information security awareness, education and training 331
A.6.4 Disciplinary process 335
A.6.5 Responsibilities after termination or change of employment 339
A.6.6 Confidentiality or non-disclosure agreements 343
A.6.7 Remote working 347
A.6.8 Information security event reporting 351

Chapter 17 **A.7 Physical controls** 355
A.7.1 Physical security perimeters 356
A.7.2 Physical entry 360
A.7.3 Securing offices, rooms and facilities 364
A.7.4 Physical security monitoring 368
A.7.5 Protecting against physical and environmental threats 372
A.7.6 Working in secure areas 376
A.7.7 Clear desk and clear screen 380
A.7.8 Equipment siting and protection 385
A.7.9 Security of assets off-premises 390
A.7.10 Storage media 395
A.7.11 Supporting utilities 399
A.7.12 Cabling security 403
A.7.13 Equipment maintenance 407
A.7.14 Secure disposal or re-use of equipment 411

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT

CHAPTER 1

Introduction to ISO/IEC 27001:2022

ISO/IEC 27001 is the international standard that specifies requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). It is published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and developed by Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 27 (Information security, cybersecurity and privacy protection). It is the only standard in the ISO/IEC 27000 family against which an organisation can be independently certified for its ISMS.

This chapter explains what the standard is for, summarises how the 2022 edition differs from its 2013 predecessor, records the 2024 climate action amendment and the transition arrangements, and sets out the purpose and intended audience of this manual.

1.1 Purpose of the standard

The standard does not prescribe a particular set of technologies or a fixed list of controls that every organisation must deploy. Instead, it defines a management system: a coordinated set of policies, processes, roles, records and decision points through which an organisation understands its information security risks and decides, in a disciplined and repeatable way, how to treat them. Its central premise is that security outcomes are more durable when they are governed by management processes than when they depend on individual effort or one-off projects.

In practical terms, an ISMS conforming to ISO/IEC 27001 enables an organisation to:

- define the boundaries of what it is protecting and why, taking account of its internal and external context and the expectations of interested parties;
- assess information security risks against criteria approved by management, and select treatments that are proportionate to those risks;
- compare its selected controls against a reference set (Annex A) so that no relevant control is overlooked, and record the outcome in a Statement of Applicability;
- allocate resources, competence and accountability for security, and communicate expectations to staff and suppliers;
- operate, monitor and measure the system, audit it internally and review it at top management level; and
- correct nonconformities and improve the system continually.

SAMPLE

The standard is deliberately generic. It applies to organisations of any size, sector or legal form, including commercial companies, public bodies, not-for-profit organisations and service providers that process information on behalf of others. The same requirements apply to a 40-person software studio and to a multinational bank; what differs is the scale, formality and complexity of the processes each organisation builds to meet them.

Why organisations adopt it

Organisations typically adopt ISO/IEC 27001 for one or more of the following reasons:

- **Customer and contractual assurance.** Enterprise customers, particularly in financial services, healthcare, government and technology outsourcing, frequently request evidence of an independently certified ISMS during supplier due diligence.
- **Regulatory alignment.** Although ISO/IEC 27001 certification is rarely mandated by law, a functioning ISMS provides a structured basis for meeting legal obligations such as those in India's Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000 and associated rules and directions, or the EU General Data Protection Regulation.
- **Governance and accountability.** Boards and executive committees use the ISMS to obtain regular, structured visibility of security risk and performance.
- **Operational discipline.** The management system disciplines (risk assessment, internal audit, corrective action) reduce reliance on informal practice and key individuals.

> **Requirement versus control.**
> ISO/IEC 27001 Clauses 4 to 10 are requirements that an organisation must meet to claim conformity. The controls in Annex A are a reference list against which the organisation compares the controls it has determined as necessary through risk treatment. An Annex A control becomes an obligation for a particular organisation only when that organisation selects it and records it as applicable in its Statement of Applicability. This distinction runs through the entire manual.

1.2 Evolution of the standard

ISO/IEC 27001 traces its lineage to British Standard BS 7799. Part 1 of that standard (a code of practice for controls) became ISO/IEC 17799 and was later renumbered ISO/IEC 27002. Part 2 (the management system specification) became ISO/IEC 27001:2005. The sec-

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT

ond edition, ISO/IEC 27001:2013, aligned the standard with the common high-level structure then used for ISO management system standards (Annex SL). The third edition, ISO/IEC 27001:2022, was published in October 2022 *[Verify exact publication date]*, following publication of the revised control guidance in ISO/IEC 27002:2022 earlier the same year.

Table 1-1. Principal editions of ISO/IEC 27001

Edition	Key characteristics
ISO/IEC 27001:2005	First international edition derived from BS 7799-2; explicit Plan-Do-Check-Act model; Annex A of 133 controls in 11 domains.
ISO/IEC 27001:2013	Adopted the Annex SL high-level structure; risk assessment no longer tied to an asset-based method; Annex A of 114 controls in 14 domains (A.5 to A.18).
ISO/IEC 27001:2022	Adopted the Harmonized Structure; modest changes to Clauses 4 to 10; Annex A aligned with ISO/IEC 27002:2022 (93 controls in 4 themes).
ISO/IEC 27001:2022/Amd 1:2024	Climate action changes to Clauses 4.1 and 4.2, applied across ISO management system standards.

1.3 What changed in the 2022 revision

The 2022 revision is best understood as two distinct sets of changes: relatively light-touch changes to the management system clauses, and a substantial restructuring of Annex A driven by the new edition of ISO/IEC 27002. The full title of the standard also changed to include the words "information security, cybersecurity and privacy protection", reflecting the renamed subcommittee.

Changes to the management system clauses (Clauses 4 to 10)

The clauses were aligned with the Harmonized Structure (HS) for ISO management system standards, the successor to Annex SL. The changes were mostly clarifications, but several have practical consequences for implementation and audit. They are summarised below in Srida IT's own words; the licensed standard remains the authoritative source.

Table 1-2. Summary of principal clause-level changes, 2013 to 2022

Clause	Nature of change	Practical implication
4.2	Adds an explicit step of determining which interested-party requirements will be addressed through the ISMS.	The interested-parties register should show not only requirements but a decision on which are in scope of the ISMS.
4.4	Wording now refers to the processes needed and their interactions, in line with the HS.	Organisations are expected to identify ISMS processes and how they connect, not merely produce documents. A process map or process inventory is useful evidence.
5.3	Clarifies that roles and responsibilities are communicated within the organisation.	Evidence of communication (not just definition) of roles is expected.
6.2	Objectives must be monitored, and documented information on them must be available.	Objectives need owners, measures and a monitoring record.
6.3	New clause on planning of changes to the ISMS.	Changes to the ISMS itself (scope, structure, key processes) should be planned and controlled, not made ad hoc.
7.4	The item on the processes by which communication is effected was simplified to how to communicate.	Communication plans should state method or channel.
8.1	Adds establishing criteria for processes and implementing control of processes in accordance with those criteria; refers to externally provided processes, products or services relevant to the ISMS.	Outsourced and cloud-delivered processes must be controlled as part of operational planning, linking Clause 8.1 to the supplier controls in A.5.19 to A.5.23.
9.1	Notes that methods should produce comparable and reproducible results.	Metrics should be defined consistently so that trends are meaningful.
9.2	Split into 9.2.1 General and 9.2.2 Internal audit programme.	Structural; requirements largely unchanged.
9.3	Split into 9.3.1, 9.3.2 and 9.3.3; adds an input on changes in the needs and expectations of interested parties.	Management review agendas and minutes should cover the new input.
10	Order of 10.1 and 10.2 reversed (continual improvement first).	Structural only.

Audit focus after transition.

In Srida IT's experience, the clause changes most often found weakly implemented after transition are 6.3 (changes made to the ISMS without any recorded planning), 8.1 (outsourced processes not identified or controlled) and 9.3 (management review minutes not evidencing the new interested-party input). Part II gives specific testing procedures for each.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT

CONTROL A.5.15

Access control

Annex A reference control · applicability per risk treatment & SoA | WP-A5.15

1 Control Identification

Attribute	Detail
Control identifier	A.5.15
Control title	Access control
Control theme	A.5 Organizational controls
Control purpose	To set the rules that decide who and what may reach information and systems, so that access is granted on business need and nothing more.
ISO/IEC 27002:2022 reference	ISO/IEC 27002:2022, 5.15
Control type†	Preventive
Security properties†	Confidentiality, Integrity, Availability
Cybersecurity concepts†	Protect
Relevant risks	• Unauthorised access to information because access rules are undefined or inconsistently applied. • Excessive privileges accumulated over time leading to fraud, error or larger breach impact. • Segregation of duties conflicts enabling a single person to initiate and approve sensitive transactions. • Default-allow configurations exposing systems to users and services that have no need for them. • Inconsistent rules across on-premises, SaaS and cloud platforms creating blind spots.

† ISO/IEC 27002:2022 attribute values as understood by Srida IT; verify against the licensed standard.

SAMPLE

CONTROL UNDERSTANDING

2 Control Objective and Intended Outcome

A documented, risk-based access control policy defines the principles, models and responsibilities for logical and physical access, and those rules are translated into role definitions and system configurations that are consistently enforced across the scope.

3 Control Description

This control is the policy layer for the access control family. Controls A.5.16 (identity management), A.5.17 (authentication information), A.5.18 (access rights), A.8.2 (privileged access rights), A.8.3 (information access restriction) and A.8.5 (secure authentication) implement it. Srida IT recommends a topic-specific access control policy that sets out: the principles of need-to-know and least privilege; default-deny; the access model (role-based, attribute-based or a combination); segregation of duties rules; how access is requested, approved, provisioned, reviewed and removed; treatment of privileged, emergency, service and third-party access; and how physical and logical access rules align. The policy should be supported by role catalogues or access matrices for key applications, showing which roles exist, what entitlements each role carries and which role combinations are prohibited.

4 Business and Security Rationale

Without agreed rules, access decisions are made one request at a time by administrators who lack business context, leading to privilege creep and inconsistent protection. A clear policy and role model make access predictable, auditable and scalable, and allow access reviews to test against a defined baseline rather than opinion.

5 Threat Scenarios Addressed

- A finance clerk retains vendor-master edit rights from a previous role and creates a fictitious supplier.
- A developer with standing production database access exfiltrates customer data.
- A newly deployed SaaS application is opened to all employees by default and exposes HR records.
- Attackers using a compromised account move laterally because network and application access is not segmented by role.
- A contractor retains broad file share permissions after the engagement ends.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT

IMPLEMENTATION

6 Applicability and Scoping

Applicable to all organisations; exclusion from the SoA cannot reasonably be justified, since every ISMS must govern who can access information. Scope should cover all in-scope applications, infrastructure, cloud tenancies, SaaS services and physical areas, and all user populations including employees, contractors, suppliers, service accounts and machine identities.

7 Implementation Guidance

1. Draft an access control policy approved by management covering principles, access models, SoD, lifecycle, privileged and emergency access, remote access, third-party access and review frequency.
2. Identify in-scope applications and platforms and rank them by criticality and sensitivity to prioritise role design.
3. For each critical application, produce an access matrix or role catalogue mapping job roles to entitlements, with a named application owner.
4. Define a segregation of duties ruleset for key business processes (procure-to-pay, order-to-cash, payroll, change deployment) and identify conflicting entitlement pairs.
5. Configure systems to default-deny and use groups or roles rather than direct user assignments wherever the platform allows.
6. Align physical access zones with logical roles so that, for example, data centre access is restricted to infrastructure roles.
7. Integrate the policy with the identity governance or IAM platform so that role definitions drive provisioning and review campaigns.
8. Define and document exceptions handling, including time-bound approval and compensating controls.
9. Review the policy at least annually and after significant organisational or technology change.

8 Roles and Responsibilities

Role	Responsibility
Top management / CISO	Approves the access control policy and risk acceptance for exceptions.
Application and system owners	Define roles and entitlements, approve access and own SoD rules for their systems.
IAM team	Implements the role model in identity platforms and maintains the access matrix tooling.
Line managers	Request access for their staff consistent with job role and need-to-know.
Internal audit / second line	Independently tests SoD and policy compliance.

9 Recommended Documented Information

- Access control policy (topic-specific policy)
- Role catalogues or access matrices for critical applications
- Segregation of duties ruleset and conflict register
- Access control exception register
- Physical access zone definitions mapped to roles

ASSESSMENT AND TESTING

10 Audit Testing Procedures

Recommended Srida IT testing methodology; not prescribed by ISO/IEC 27001 or ISO/IEC 27002.

Table 15-16. Audit testing procedures, Control A.5.15

Test ID	Method	Testing procedure	Result
TP-A.5.15-01	EXAMINE	Examine the access control policy and verify that it is approved, current and addresses need-to-know, least privilege, default-deny, access models, segregation of duties, privileged, emergency, third-party and service access, and review frequency.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.5.15-02	EXAMINE	Examine access matrices or role catalogues for a sample of critical applications and verify that each role has a defined set of entitlements, a named owner and is linked to job functions.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.5.15-03	EXAMINE	Examine the segregation of duties ruleset and verify that conflicts are defined for key business processes and that a mitigating control is documented for each accepted conflict.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.5.15-04	INSPECT	Inspect user-to-entitlement exports from a sample of critical applications and verify that access is granted through roles or groups and that direct assignments are limited and justified.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT

Test ID	Method	Testing procedure	Result
TP-A.5.15-05	**RE-PERFORM**	Run the SoD ruleset against current user entitlement exports for in-scope financial and operational systems and verify that no unmitigated conflicts exist.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.5.15-06	**SAMPLE**	Select a sample of users across job roles and compare their actual entitlements to the access matrix for their role, and verify that any excess entitlement is approved and documented.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.5.15-07	**SAMPLE**	Select a sample of entries from the access control exception register and verify that each has a business justification, an expiry date, compensating controls and an approver of appropriate authority.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-A.5.15-08	**INTERVIEW**	Interview application owners and verify that they understand their responsibility for role design, approvals and SoD in their applications.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A

11 Sampling Guidance

Select 3–5 critical applications (for example ERP, core banking or production cloud tenancy, HR system, customer database) for role design testing. For role-to-entitlement comparison, sample 25–40 users across those applications weighted to sensitive roles. Run SoD analysis on the full population where data allows rather than sampling. For exceptions, test all if fewer than 25, otherwise 25.

12 Interview Questions

Interviewee	Question
CISO	How does the access control policy decide between role-based and attribute-based access, and where is each used?
ERP application owner	Which role combinations are prohibited in your system and how would you know if someone held both?
IAM lead	What proportion of entitlements are assigned directly to users rather than through roles or groups?
Line manager	How do you decide what access to request for a new team member?

13 Technical Verification

- Export Active Directory / Entra ID group memberships and compare to role definitions.
- Run SoD conflict analysis (for example via ERP GRC module, IGA tool or scripted comparison) on full entitlement datasets.
- Query cloud IAM for policies granting wildcard actions or resources (for example Action:* or roles/owner at organisation level).
- Check SaaS admin consoles for default sharing and default access settings.
- Compare physical access card groups with logical infrastructure roles.

14 Expected Audit Evidence

- Approved access control policy with review history
- Role catalogues or access matrices
- SoD ruleset and conflict analysis output
- Entitlement exports from sampled systems
- Exception register with approvals
- Interview notes with application owners

15 Evaluation Criteria

Effective

- Policy is comprehensive and approved; role models exist for critical systems and are used to provision access.
- SoD conflicts are defined, monitored and either resolved or formally mitigated.
- Sampled users' access is consistent with their roles.

Partially effective

- Policy exists but role definitions are missing for some critical systems.
- SoD rules defined but not periodically tested.

Ineffective

- No access control policy, or policy not reflected in system configuration.
- Widespread direct assignments and unmitigated SoD conflicts.

16 Common Gaps and Nonconformities

- Policy is generic and not supported by any role definitions.
- SoD considered only for finance systems, not for IT change and deployment.

© 2026 Srida IT · Version 1.0 · Independent guidance, not an official ISO/IEC publication

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT

- Example nonconformity: The access control policy requires access to be granted on least privilege. In the cloud production account, 14 of 22 engineering users hold the AdministratorAccess policy with no documented justification; the role catalogue defines only two administrative roles.
- Exceptions granted without expiry and never revisited.
- Third-party and service account access not addressed in the policy.

17 Remediation Guidance

- Develop role catalogues for critical applications with owners and SoD rules.
- Migrate direct assignments to role or group-based access.
- Introduce automated SoD detection through the IGA platform or scheduled scripts.
- Add expiry and periodic re-approval to all access exceptions.
- Extend the policy to cover service, machine and third-party identities explicitly.

18 Monitoring Metrics

- Percentage of critical applications with an approved role catalogue
- Number of unmitigated SoD conflicts
- Percentage of entitlements assigned via roles or groups
- Number of expired, unremediated access exceptions

19 Control Maturity Indicators

Initial	Defined	Managed	Optimised
Access granted ad hoc on request; no written policy.	Policy approved and roles defined for some systems; SoD considered informally.	Roles defined for all critical systems, provisioned through IAM, SoD monitored and exceptions time-bound.	Policy-as-code and attribute-based conditions applied consistently, with continuous entitlement analytics detecting drift.

SAMPLE

20 Related Clauses and Controls

- A.5.16 Identity management
- A.5.18 Access rights
- A.5.3 Segregation of duties
- A.8.2 Privileged access rights
- A.8.3 Information access restriction
- A.7.2 Physical entry

21 Implementation Example

> A 600-employee fintech defined an access control policy built on role-based access for business applications and attribute-based conditions (device compliance, location) for its cloud console. It produced role catalogues for its lending platform, ERP and AWS organisation, each owned by the relevant head of function. An SoD ruleset of 28 conflict pairs was loaded into its identity governance tool, which flagged two existing conflicts in loan disbursement; one was resolved and one accepted with a weekly maker-checker report reviewed by the finance controller.

22 Auditor Workpaper Reference

WP-A5.15: use the workpaper template in Appendix F.

© 2026 Srida IT · Version 1.0 · Independent guidance, not an official ISO/IEC publication

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT

CONTROL A.5.16

Identity management

Annex A reference control · applicability per risk treatment & SoA | WP-A5.16

1 Control Identification

Attribute	Detail
Control identifier	A.5.16
Control title	Identity management
Control theme	A.5 Organizational controls
Control purpose	To ensure every person and system that accesses the organisation's resources has a unique, accountable identity that is managed from creation to removal.
ISO/IEC 27002:2022 reference	ISO/IEC 27002:2022, 5.16
Control type†	Preventive
Security properties†	Confidentiality, Integrity, Availability
Cybersecurity concepts†	Protect
Relevant risks	• Shared or generic accounts that make actions untraceable to an individual. • Orphaned accounts left active after a person leaves or a system is decommissioned. • Duplicate identities for the same person across directories, creating unmanaged access. • Service accounts and machine identities created without an owner, often with high privilege and non-expiring credentials. • Identities created without verification, enabling impostors or fictitious users.

† ISO/IEC 27002:2022 attribute values as understood by Srida IT; verify against the licensed standard.

SAMPLE

CONTROL UNDERSTANDING

2 Control Objective and Intended Outcome

Each human, service and machine identity in scope is unique, linked to an accountable owner and an authoritative source, verified before creation, and disabled or removed promptly when no longer needed, with shared identities permitted only by documented exception.

3 Control Description

Identity management covers the full lifecycle of identities, distinct from the rights attached to them (A.5.18). Srida IT recommends that the HR system be the authoritative source for employee identities and a contractor or vendor register be the source for non-employees, feeding the central directory (for example Active Directory, Entra ID, Okta) through automated provisioning. Each identity should carry attributes such as unique ID, manager, department, employment type and end date. Non-human identities (service accounts, API keys bound to applications, workload identities, bots and RPA users) require an owner, purpose, and periodic attestation. Shared accounts should be avoided; where unavoidable (for example a break-glass account or a legacy system), they need explicit approval, credential vaulting and logging that attributes use to an individual.

4 Business and Security Rationale

Every other access control depends on knowing who is acting. Unique, well-governed identities make accountability, logging, access review and incident investigation possible, and timely deprovisioning removes one of the most common routes for unauthorised access.

5 Threat Scenarios Addressed

- A former employee logs in to a SaaS tool weeks after leaving because the account was not federated to the directory.
- Attackers compromise a dormant service account with a non-expiring password and domain admin rights.
- A shared 'admin' account on a firewall is used to make an unauthorised change that cannot be attributed.
- A fictitious contractor identity is created to obtain system access.
- Duplicate accounts for the same user evade quarterly access reviews.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27001 · © 2026 Srida IT