SRIDA IT PROFESSIONAL REFERENCE PUBLICATION

NIST CSF 2.0

NIST Cybersecurity Framework 2.0 · with an India lens

Implementation Guidance & Assessment Testing Procedures

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

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

Independent professional guidance.
Not a NIST publication.

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



NIST Cybersecurity Framework (CSF) 2.0 — with an India Lens

Implementation Guidance & Assessment Testing Procedures

SAMPLE

Prepared by

Rajendra Bodda

Chief Information Security Officer (CISO)

Published by Srida IT
SRIDA-NIST-CSF-RTP-001 · Version 1.0 · November 2026

This publication is an independently developed professional guidance document prepared by Srida IT. It is not a publication of the National Institute of Standards and Technology (NIST) or of any Indian regulator, is not endorsed by NIST, is not legal advice, and does not confer any certification: there is no NIST CSF certification. Only NIST CSWP 29 as published by NIST is the authoritative text of CSF 2.0.

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

Document Information and Control

Field	Value
Document title	NIST Cybersecurity Framework (CSF) 2.0 — with an India Lens
Subtitle	Implementation Guidance & Assessment Testing Procedures
Document identifier	SRIDA-NIST-CSF-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	November 2026
Reference document	National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Paper (CSWP) 29, 26 February 2024, https://doi.org/10.6028/NIST.CSWP.29
Related documents	ISO/IEC 27001:2022; NIST SP 800-53 Rev. 5; NIST SP 800-161r1; CIS Critical Security Controls v8; CERT-In Directions of 28 April 2022; SEBI CSCRF (2024); DPDP Act 2023 and DPDP Rules 2025
Companion publications	SRIDA-ISMS-27001-RTP-001; SRIDA-AIMS-42001-RTP-001; SRIDA-DPDP-RTP-001; SRIDA-CERTIN-AISA-RTP-001
Next review	On a new CSF version or significant NIST resource update, 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)	10 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.

© 2026 Srida IT · Version 1.0 · Independent guidance, not a NIST publication

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

Table of Contents

Part I Foundations 13

Chapter 1 Introduction to NIST CSF 2.0 14
Chapter 2 Structure: Core, Profiles, Tiers and NIST Online Resources 18
Chapter 3 CSF Tiers in Depth 23
Chapter 4 Organizational and Community Profiles 29
Chapter 5 CSF and Related Frameworks 34
Chapter 6 Terminology and Abbreviations 39
Chapter 7 How to Use This Manual and the Assessment Method 44

Part II The CSF Core 48

Chapter 8 Govern (GV) 49
GV.OC Organizational Context 50
GV.RM Risk Management Strategy 59
GV.RR Roles, Responsibilities, and Authorities 69
GV.PO Policy 77
GV.OV Oversight 85
GV.SC Cybersecurity Supply Chain Risk Management 92
Chapter 9 Identify (ID) 105
ID.AM Asset Management 106
ID.RA Risk Assessment 115
ID.IM Improvement 125
Chapter 10 Protect (PR) 132
PR.AA Identity Management, Authentication, and Access Control 133
PR.AT Awareness and Training 143
PR.DS Data Security 150
PR.PS Platform Security 159
PR.IR Technology Infrastructure Resilience 169
Chapter 11 Detect (DE) 176
DE.CM Continuous Monitoring 177
DE.AE Adverse Event Analysis 186
Chapter 12 Respond (RS) 195
RS.MA Incident Management 196
RS.AN Incident Analysis 206
RS.CO Incident Response Reporting and Communication 214
RS.MI Incident Mitigation 222
Chapter 13 Recover (RC) 229
RC.RP Incident Recovery Plan Execution 230
RC.CO Incident Recovery Communication 240

Part III Implementation 247

Chapter 14 Implementation Roadmap: Profile-Driven, Step by Step 248
Chapter 15 Cybersecurity Risk Governance and Board Reporting 254
Chapter 16 Cybersecurity Supply Chain Risk Management in Practice 259
Chapter 17 Measurement, Metrics and Continuous Improvement 264

SAMPLE

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

Chapter 18	One Control Set: CSF with ISO/IEC 27001 and Indian Regulations	269
Chapter 19	CSF for Small and Medium Enterprises	274
Part IV	**Assessment**	**278**
Chapter 20	CSF Assessment Programme	279
Chapter 21	Assessment Techniques and Evidence	284
Chapter 22	Findings, Gap Reports and Executive Reporting	289
Part V	**Appendices and Templates**	**295**
Appendix A	Subcategory Matrix	296
Appendix B	Category Summary	301
Appendix C	Organizational Profile Template	302
Appendix D	Tier Assessment Worksheet	310
Appendix E	Gap Analysis and Action Plan Template	314
Appendix F	CSF 2.0 to ISO/IEC 27001:2022 Crosswalk	318
Appendix G	India Regulatory Touchpoints Matrix	325
Appendix H	Assessment Workpaper and Completed Sample	329
Appendix I	Board Reporting Template	335
Appendix J	References	338

SAMPLE

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

CHAPTER 1

Introduction to NIST CSF 2.0

The NIST Cybersecurity Framework (CSF) 2.0 is a short publication with a large footprint. Published by the US National Institute of Standards and Technology on 26 February 2024 as NIST Cybersecurity White Paper (CSWP) 29, it sets out a catalogue of cybersecurity outcomes that any organisation can use to understand where it stands, decide where it needs to be, and explain both positions to the people who fund, oversee and depend on it. This chapter explains what the CSF is for, what it is not, who uses it, how version 2.0 differs from its predecessors and why Indian organisations increasingly meet it in contracts, client questionnaires and regulatory conversations.

The manual that follows is written for practitioners who must implement the CSF and for assessors who must test whether its outcomes are being achieved. It is a Srida IT publication. It does not reproduce the CSF, and it is not a NIST document; readers should keep CSWP 29 itself at hand and treat it as the only authority for what the Framework says.

1.1 Purpose of the Framework

The CSF exists to help organisations manage cybersecurity risk. It does this by offering a common vocabulary of high-level outcomes, arranged in a hierarchy, rather than a list of technical controls. NIST describes the Core as “a taxonomy of high-level cybersecurity outcomes”, and the choice of the word "taxonomy" is deliberate: the CSF classifies what good cybersecurity risk management achieves, and leaves the method of achieving it to the organisation.

NIST identifies four broad uses. An organisation can use the CSF to **understand** and **assess** its posture, describing its current or desired state for all or part of the business and measuring progress in closing the gaps between them. It can use the Framework to **prioritise** actions in line with its mission, legal obligations and risk appetite. And it can use the CSF to **communicate**, internally between practitioners, managers and executives, and externally with clients, suppliers, regulators and partners. Of these, communication is often the most valuable in practice. A board that cannot read a vulnerability report can still follow a discussion framed around whether the organisation reliably detects and responds to incidents.

SAMPLE

Three components make up the Framework:

- **The CSF Core** — six Functions, 22 Categories and 106 Subcategories of outcomes (Chapter 2 and Part II).
- **CSF Organizational Profiles** — a way of describing an organisation's current and/or target posture in terms of Core outcomes (Chapter 4).
- **CSF Tiers** — four characterisations of how rigorous an organisation's cybersecurity risk governance and management practices are (Chapter 3).

Around these components NIST maintains a suite of online resources — Informative References, Implementation Examples, Quick-Start Guides and Community Profiles — which are updated more often than the Framework itself. Chapter 2 describes them.

1.2 A voluntary, outcome-based framework

The CSF is voluntary. NIST notes that it may be adopted voluntarily or through governmental policies and mandates, which means that a government or regulator can choose to require its use; the Framework itself imposes no obligation on anyone. No certification scheme exists for the CSF: there is no accredited certification body, no certificate of conformity and no NIST register of "CSF-compliant" organisations. A claim that an organisation has been "certified" against the CSF should be treated as a misstatement. What an organisation can legitimately say is that it has assessed itself, or been assessed by an independent party, against the CSF outcomes, and that the assessment produced a particular Current Profile and Tier characterisation as at a stated date and for a stated scope.

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

No certification exists

This manual uses the language of assessment, not certification. Assessments performed with it produce a documented view of which Subcategory outcomes are achieved, partially achieved or not achieved, with evidence. They do not produce a certificate, and an assessment report should never be presented as one. Where a client asks for a CSF "certificate", the right response is to explain what an independent CSF assessment can and cannot show, and, if formal certification is the real need, to discuss ISO/IEC 27001.

The CSF is also outcome-based. Each Subcategory states a result — for example, that inventories of hardware are maintained, or that incidents are contained — and does not say how the result should be achieved, by whom, or with what technology. NIST is explicit that the outcomes are not a checklist of actions and that the order and size of the Functions, Categories and Subcategories say nothing about sequence or importance. Two organisations can achieve the same outcome in very different ways: a 40-person Bengaluru SaaS start-up may meet the asset inventory outcome with a cloud provider's resource inventory and a spreadsheet of laptops, while a Chennai auto-parts manufacturer with operational technology (OT) may need passive network discovery across plant networks and an engineering-maintained register of programmable logic controllers.

For the assessor, outcome-based design has a direct consequence. The question is never "does the organisation have control X?" but "does the evidence show that this outcome is achieved, to the extent the organisation's risk requires?" This is why Part II pairs each outcome with testing procedures, evaluation criteria and evidence lists rather than with a fixed control specification.

1.3 Audience: well beyond critical infrastructure

The first two versions of the Framework carried the title “Framework for Improving Critical Infrastructure Cybersecurity”. That title has been dropped for 2.0. The change recognises what had already happened in practice: the Framework was being used by organisations of every size and sector, in many countries, whether or not they operated critical infrastructure. CSF 2.0 states that it is intended for industry, government, academia and non-profit organisations, regardless of the maturity of their cybersecurity programmes.

SAMPLE

NIST names the primary audience as the people responsible for developing and leading cybersecurity programmes. It also lists a wider group who make decisions with cybersecurity consequences: executives, boards of directors, procurement professionals, technology staff, risk managers, lawyers, human resources specialists and auditors. Finally it recognises policy makers and influencers — associations, professional bodies and regulators — who set and communicate cybersecurity priorities. This manual serves all three groups, with Part II and Part IV aimed principally at practitioners and assessors, and Chapter 15 and Appendix I aimed at boards and executives.

1.4 From 1.0 and 1.1 to 2.0

The Framework has a history of roughly a decade. Version 1.0 was published in February 2014 following a US Executive Order on improving critical infrastructure cybersecurity, and was developed with extensive industry participation. Version 1.1 followed in April 2018 and added, among other things, more material on supply chain risk management, identity and authentication, and self-assessment. Version 1.1 had five Functions — Identify, Protect, Detect, Respond and Recover — with 23 Categories and 108 Subcategories.

Version 2.0 was the product of a multi-year revision involving public comment, workshops and draft releases. It keeps the overall architecture — Core, Profiles and Tiers — but changes a great deal within it.

Table 1-1. Principal changes from CSF 1.1 to CSF 2.0

Area	CSF 1.1 (summary)	CSF 2.0	Practical effect
Title and scope	Framed around critical infrastructure	Title shortened; explicitly for all organisations, sectors and sizes	Removes the perception that the CSF is only for utilities, telecoms or banks
Functions	Five Functions	Six Functions, with GOVERN added at the centre	Governance outcomes become assessable in their own right rather than scattered

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

CHAPTER 8

Govern (GV)

GOVERN establishes and monitors the organisation's cybersecurity risk management strategy, expectations and policy. It is new as a separate Function in CSF 2.0 and informs how the other five are prioritised and carried out. The GOVERN Function has 6 Categories and 31 Subcategories. Each entry follows the format described in Chapter 7.

Table 8-1. Categories in the GOVERN Function

Category	Title	Subcategories	Tests	Workpaper
GV.OC	Organizational Context	5	13	WP-GV.OC
GV.RM	Risk Management Strategy	7	16	WP-GV.RM
GV.RR	Roles, Responsibilities, and Authorities	4	12	WP-GV.RR
GV.PO	Policy	2	11	WP-GV.PO
GV.OV	Oversight	3	11	WP-GV.OV
GV.SC	Cybersecurity Supply Chain Risk Management	10	16	WP-GV.SC

SAMPLE

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

CSF 2.0 CATEGORY GV.OC · GOVERN (GV) FUNCTION · 5 SUBCATEGORIES

Organizational Context

CSF outcome · voluntary framework | WP-GV.OC

A Category Reference and Subcategories

NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, 26 February 2024, Category GV.OC — Organizational Context

"The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood"

Outcome statements are quoted from CSF 2.0; explanations are in Srida IT's own words. Subcategories describe outcomes, not controls.

Table 8-2. Subcategories of GV.OC Organizational Context

Subcategory	CSF 2.0 outcome (NIST wording)	What it means in practice (Srida IT)
GV.OC-01	**"The organizational mission is understood and informs cybersecurity risk management"**	The organisation knows what it exists to do, and that purpose visibly shapes how cybersecurity risk is identified, prioritised and accepted.
GV.OC-02	**"Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered"**	The people and bodies with an interest in the organisation's cybersecurity, inside and outside, are identified, and what they need and expect is captured and taken into account in risk decisions.
GV.OC-03	**"Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed"**	The laws, regulations and contract terms that impose cybersecurity obligations, including obligations on privacy and civil liberties, are identified, kept current and actively managed through owners and controls.
GV.OC-04	**"Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated"**	The organisation knows which of its objectives, capabilities and services others rely on or expect, and it tells the relevant parties what it will deliver and at what level of resilience.
GV.OC-05	**"Outcomes, capabilities, and services that the organization depends on are understood and communicated"**	The organisation knows which external and internal outcomes, capabilities and services it relies on to operate, and that dependency information is shared with those who make risk decisions.

© 2026 Srida IT · Version 1.0 · Independent guidance, not a NIST publication

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

B Implementation Examples (Srida IT)

Subcategory	Practical examples
GV.OC-01	• The cybersecurity strategy opens with a one-page statement linking the business mission (for example, uninterrupted loan disbursal for an NBFC) to the security priorities that protect it. • Risk assessment criteria weight impact on mission-critical activities more heavily than impact on supporting activities. • Each annual security plan item is traced to a mission objective or business outcome in the board-approved strategy.
GV.OC-02	• A stakeholder register lists customers, regulators, the board, employees, auditors, key suppliers and CERT-In as an external authority, with their security expectations and how each is engaged. • Customer security questionnaires and contractual clauses are analysed yearly and recurring expectations are fed into the Target Profile. • Employee and works-council concerns about monitoring are recorded and considered when designing endpoint telemetry.
GV.OC-03	• A legal and regulatory obligations register records each requirement (for example, CERT-In incident reporting timelines, DPDP safeguards, sector regulator directions), its source, owner, applicable systems and the control that meets it. • Legal counsel and the compliance team run a quarterly horizon scan for new circulars and directions and log the impact assessment. • Customer contracts are screened at signature for security clauses (breach notification windows, audit rights, data location) and these are added to the register.
GV.OC-04	• A business impact analysis identifies externally relied-upon services (for example, UPI payment collection, patient record access) with maximum tolerable downtime and recovery objectives. • Service commitments to customers and regulators are documented in service catalogues and SLAs and are consistent with the recovery capability actually tested. • Critical-service owners brief the incident response team on which outages trigger customer or regulator communication.
GV.OC-05	• A dependency map links each critical service to the cloud regions, SaaS platforms, telecom links, power supply and outsourced teams it needs. • Concentration risk is recorded where several critical services rely on a single provider or a single data centre. • Dependency information is given to procurement, business continuity and the C-SCRM function so that supplier criticality ratings are consistent.

Srida IT examples. NIST publishes its own Implementation Examples online; they are not reproduced here.

C Tier Characteristics for this Category

Tier 1 · Partial	Tier 2 · Risk Informed	Tier 3 · Repeatable	Tier 4 · Adaptive
Context is implicit and held in a few people's heads. Legal and contractual obligations are discovered when an auditor, customer or regulator raises them. Priorities are set case by case without reference to mission or dependencies. (Indicative only; Tiers characterise the overall rigour of risk governance, not a score for this Category.)	Management has documented the mission link and the main obligations, and these inform some security priorities, but the context is not maintained as organisation-wide practice. Stakeholder expectations and dependencies are known for some business units or systems only.	Context is captured through approved, recurring processes: an obligations register with owners, a stakeholder register, a business impact analysis and a dependency map that are reviewed on a schedule and on defined triggers. Changes in regulation, business model or technology lead to documented updates that flow into risk assessment and the Target Profile.	Context is continuously refreshed using regulatory horizon scanning, customer and supplier intelligence and operational data (for example, live service-dependency telemetry). Executives use the context when weighing cybersecurity alongside financial and operational risk, and the organisation adjusts priorities quickly when context shifts.

Indicative only. CSF Tiers characterise the rigour of an organisation's overall risk governance and management practices; they are not scores for individual Subcategories.

© 2026 Srida IT · Version 1.0 · Independent guidance, not a NIST publication

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

D ISO/IEC 27001:2022 Crosswalk

- GV.OC-01 → Clause 4.1 (understanding the organisation and its context); Clause 5.1 a) (policy and objectives compatible with strategic direction); Clause 6.2 (information security objectives)
- GV.OC-02 → Clause 4.2 (needs and expectations of interested parties); Clause 7.4 (communication)
- GV.OC-03 → Clause 4.2 c) (requirements to be addressed through the ISMS); Annex A 5.31 (legal, statutory, regulatory and contractual requirements), 5.32 (intellectual property rights), 5.33 (protection of records), 5.34 (privacy and protection of PII), 5.36 (compliance with policies, rules and standards)
- GV.OC-04 → Clause 4.3 (scope of the ISMS); Annex A 5.29 (information security during disruption), 5.30 (ICT readiness for business continuity)
- GV.OC-05 → Clause 4.3 c) (interfaces and dependencies with other organisations); Annex A 5.19 (information security in supplier relationships), 5.21 (managing information security in the ICT supply chain), 5.23 (information security for use of cloud services), 5.30 (ICT readiness for business continuity)
- Note: ISO/IEC 27001 clause 4 is narrower than GV.OC on stakeholder expectations of service delivery; ISO 22301 clause 4 and its business impact analysis requirements are often a closer fit for GV.OC-04/05.

Indicative Srida IT mapping. Achieving a CSF outcome does not by itself establish ISO/IEC 27001 conformity, or the reverse.

E Other Framework Mappings

- NIST SP 800-53 Rev. 5: PM (Program Management) family, notably mission and business process definition and critical infrastructure planning; CP (Contingency Planning) for business impact analysis; SR (Supply Chain Risk Management) for dependencies
- NIST IR 8286 series (cybersecurity and ERM) and IR 8286D (business impact analysis) for linking mission and impact
- NIST SP 800-221 / 800-221A for placing ICT risk within the enterprise risk portfolio
- NIST Privacy Framework (for privacy and civil liberties obligations under GV.OC-03)
- CIS Controls v8: Control 15 (Service Provider Management) supports GV.OC-05; CIS v8 has no direct equivalent for mission or stakeholder analysis
- ISO 22301:2019 clauses 4.1–4.2 and 8.2 (business impact analysis and risk assessment) for GV.OC-04/05

F India Regulatory Touchpoints

- CERT-In Directions under section 70B(6) of the IT Act, dated 28 April 2022: obligations (reporting specified incidents within 6 hours, maintaining logs for 180 days within Indian jurisdiction, synchronising clocks to specified NTP sources, nominating a point of contact) belong in the GV.OC-03 obligations register for service providers, intermediaries, data centres, body corporates and government organisations.
- Digital Personal Data Protection Act 2023, s.8(5) (reasonable security safeguards to prevent personal data breach) and the DPDP Rules 2025 on security safeguards and breach intimation (r.6 and r.7) are privacy-related cybersecurity obligations under GV.OC-03; applicability and commencement dates of individual provisions should be confirmed.
- Sector regulators: SEBI Cybersecurity and Cyber Resilience Framework (CSCRF, 2024) for SEBI-regulated entities, RBI directions on IT governance, risk, controls and assurance and on cyber security for banks and NBFCs, and IRDAI information and cyber security guidelines for insurers each add obligations and define critical services for GV.OC-03/04.
- Entities notified as Critical Information Infrastructure or protected systems under s.70 of the IT Act and NCIIPC guidance face additional expectations that shape GV.OC-04. Mapping these obligations to CSF outcomes is a management aid; it does not by itself demonstrate compliance.

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

G Objective

Organizational Context establishes the facts on which every other cybersecurity decision rests. Before an organisation can decide how much risk to accept, which assets to protect first or which suppliers matter most, it has to understand its mission, the people and institutions with an interest in how it handles cybersecurity, the legal and contractual obligations it carries, the services others depend on it to provide, and the services it depends on in turn. In CSF 2.0 these are expressed as outcomes under GOVERN, and they feed the risk management strategy (GV.RM), policy (GV.PO), supply chain risk man-

SAMPLE

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

agement (GV.SC) and the scoping of every Organizational Profile. The Category is achieved when this context is documented, current, owned and demonstrably used, not merely written down once for an audit.

H Interpretation

CSF outcome. The Category describes an understanding, not a document. NIST frames it as the circumstances "surrounding the organization's cybersecurity risk management decisions" being understood. An assessor therefore looks for two things: a reasonable, current articulation of context, and evidence that the articulation influences decisions such as risk ratings, investment choices, recovery objectives and supplier tiering. A beautifully written context statement that nobody consulted when setting the year's priorities is a design that has not operated.

What good looks like varies with size and sector. A 40-person Bengaluru SaaS start-up may hold its entire context in a few pages: mission, top customers and their contractual security asks, the obligations that apply (CERT-In Directions, DPDP Act duties as a Data Fiduciary or Processor, customer-imposed SOC 2 or ISO/IEC 27001 expectations), the services it promises, and the cloud and SaaS stack it depends on. A listed Mumbai bank or a SEBI-regulated market infrastructure institution will need a formal obligations register maintained by compliance, a board-approved business impact analysis, and dependency mapping that reaches into fourth parties. Both can achieve the outcome; the rigour should be proportionate to the consequences of getting the context wrong.

IT and OT. For a Chennai auto-parts manufacturer the mission is to ship conforming parts on schedule to vehicle makers who run just-in-time lines. Its context must therefore include OT dependencies (PLCs, SCADA historians, vendor remote access, power quality), safety obligations under factory law, and customer expectations that may be expressed through industry supplier-assessment schemes. Context work that covers only the corporate IT estate will understate both the services others rely on (GV.OC-04) and the services the plant relies on (GV.OC-05).

Common misreadings. First, treating GV.OC-03 as a list of laws rather than a managed set of obligations with owners, applicability and linked controls. Second, confusing GV.OC-04 and GV.OC-05: the first faces outward (what others need from us), the second faces inward (what we need from others). Third, assuming context is static: mergers, a new product line, a new regulator, or a move to a different cloud provider all change it, so the outcome includes a trigger-based refresh. Fourth, believing that a statement of applicability or ISMS scope document alone achieves the Category; it is a useful input but rarely captures stakeholder expectations or dependency criticality in enough depth.

SAMPLE

I Applicability

Every organisation that uses the CSF needs this Category, because it scopes everything else. Depth should follow consequence. A small organisation can meet the outcome with a short context statement, a one-page obligations list maintained by a named owner, and a simple dependency table showing its cloud host, payment gateway, email platform and managed service provider. Regulated financial entities, hospitals, CII operators and listed companies should expect a formal obligations register reviewed by compliance and legal, a board-noted business impact analysis, and dependency mapping that reaches into significant fourth parties. Where operations are outsourced or cloud-hosted, the organisation still owns its context: the provider's certifications and shared-responsibility documentation are inputs to GV.OC-05, not a substitute for the organisation's own understanding of what it depends on and what it promises its own customers.

J Implementation Guidance

1. Appoint an owner for organisational context (commonly the CISO working with the risk, compliance and strategy functions) and agree a review cycle and change triggers.
2. Write a short mission-to-security statement: the organisation's mission and strategic objectives, the activities most critical to them, and the cybersecurity implications. Have it endorsed by executive management.
3. Build a stakeholder register covering internal and external parties (board, staff, customers, regulators, CERT-In, investors, insurers, key suppliers, community) with their cybersecurity expectations, the evidence source and the engagement channel.
4. Build or refresh the legal, regulatory and contractual obligations register: requirement, source, applicability, owner, linked policy and control, evidence, status. Include privacy and civil-liberty obligations and contractual security clauses.
5. Run or update a business impact analysis to identify the services others rely on, with tolerable downtime, recovery time and recovery point objectives, and confirm these are communicated to customers, regulators and the incident response and continuity teams.
6. Map inbound dependencies for each critical service: cloud and SaaS providers, telecom, power, outsourced operations, key personnel and internal shared services. Record single points of failure and concentration risk.

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