Annex G — Extended Question Catalogue
(Version 1.0 — Expandable Question Framework for NIRMATA Assessments)

Executive Overview

Annex G introduces the **Extended Question Catalogue (EQC)** and the standardized **Scoring Framework** that together operationalize the NIRMATA maturity model into a quantitative, evidence-driven system. The EQC expands each of the twelve pillars into a structured set of 12 weighted questions, aligned with the DPDP Act 2023, CERT-In 2022, ISO 27001/27701/42001, and NIST CSF 2.0. Each question links to verifiable evidence and includes a 0–5 maturity scale to ensure repeatable scoring and audit traceability.

Complementing the EQC, the Scoring Framework defines how responses, weights, and normalization produce consistent pillar-level and composite maturity indices.
This transforms self-assessment into a **data-backed benchmarking process** capable of measuring improvement over time, across sectors, and against national baselines.
By embedding transparent weighting, normalization, and verification rules, Annex G ensures that TRUST-IN Bharat assessments remain objective, comparable, and defensible—strengthening the reliability of India's cybersecurity and privacy maturity measurement ecosystem.

1. Purpose and Context

The Extended Question Catalogue (EQC) defines the authoritative library of assessment questions forming the quantitative backbone of the NIRMATA Framework under the TRUST-IN Bharat Programme. It is designed to ensure that every maturity evaluation—from self-assessment to verified audit—achieves **depth, consistency, and traceability** across sectors and over time.

This Annex formalizes the EQC's structure, governance, and review model while leaving the actual question dataset (CSV/JSON) as a separately version-controlled attachment.

Purpose

Annex G serves as the operational companion to the NIRMATA Framework. It provides detailed self-assessment questions, evidence expectations, and scoring guidance for each of the twelve domains defined in the Framework.

While the core whitepaper establishes the maturity model, governance principles, and cross-framework alignment, Annex G translates these into measurable actions and evidence points for assessors and organizations.

Living Document

Annex G is a living document maintained separately to reflect emerging threats, new regulatory references, and best-practice evolution.

Its revision cadence is independent of the Framework's core version so that new or refined question sets can be introduced without altering the foundational maturity definitions.

Each release of Annex G will clearly state the Framework version it aligns with (for example, "Annex G v1.1 — Aligned with Framework v1.0").

Access and Updates

The latest version of Annex G is available at:

https://github.com/trustin-bharat/nirmata-framework/annexes/annex-g.md

and in formatted form on the official TRUST-IN Bharat site:

https://trustin-bharat.github.io

Revision Notes

Changes to Annex G will be announced through official release notes under the "Annex G Updates" section, with a clear summary of added or modified questions and any impact on scoring weightage.

Organizations using the Framework for certification or benchmarking should periodically verify that they are using the most recent compatible version.

Attribution

2. Design Objectives

Objective	Explanation
Comprehensive Coverage	Span all control phases: policy, implementation, monitoring, improvement.
Cross-Framework Alignment	Each item references equivalent clauses in DPDP 2023, CERT-In 2022, ISO 27002 / 27701 / 42001, and NIST CSF 2.0.
Evidence Orientation	Define what constitutes acceptable objective proof for each response.
Weighted Scoring	Allow calibrated influence of each control on overall pillar maturity.
Sector Flexibility	Permit domain-specific sub-catalogues (Manufacturing, BFSI, Healthcare, Public Sector, Education).
Machine Readiness	Maintain structured metadata fields for portal ingestion and analytics.
Living Framework	Support continuous updates to reflect evolving threats, technologies, and regulatory norms.

3. Standard Data Structure

Each EQC record shall include the following core fields.
(Complete CSV and JSON schemas are provided as separate attachments for implementation.)

Field	Description	Example

Field	Description	Example
`pillar_code`	Identifier for one of the twelve NIRMATA pillars	`IR` (Incident Readiness)
`question_id`	Unique sequential ID	`IR-Q05`
`control_ref`	Linked control references	`ISO 27002 6.1.2; DPDP Sec 9(2)`
`question_text`	The actual assessment question	"Are incident categories defined with impact levels and response timelines?"
`evidence_examples`	Illustrative acceptable artefacts	"Incident Response Policy, Drill Report, Escalation Matrix"
`maturity_scale`	Descriptive 0–5 maturity anchors	"0 = Absent … 5 = Fully tested and reviewed quarterly"
`weight`	Relative importance (1–5)	`3`
`sector_tags`	Optional domain applicability	`manufacturing, BFSI`
`review_cycle`	Update interval (in months)	`12`
`last_reviewed_by`	Reviewing authority	"NIRMATA Editorial Board 2025-Q4"

4. Question Volume and Distribution

Pillar	Target Core Questions	Sector Add-ons	Evidence Prompts (min)
Governance & Leadership	12	5	6
Risk & Compliance	12	5	6
Asset & Data Management	12	4	5
Identity & Access	12	4	5
Infrastructure Security	12	4	5
Application & Product Security	12	4	5
Monitoring & Detection	12	4	5
Incident Readiness	12	4	5
Business Continuity & Resilience	12	3	4
Privacy & Data Protection	12	4	5
Supply-Chain Security	12	3	4

Pillar	Target Core Questions	Sector Add-ons	Evidence Prompts (min)
Culture, Training & Awareness	12	3	4
Total (Core)	**144**	—	—

The EQC aims for an average of **12–15 questions per pillar**, supported by evidence prompts to ensure reliability and comparability of maturity scores.

5. Governance and Revision

Cycle	Activity	Responsible Body	Output
Annual (Q4)	Review for clarity, redundancy, and weight calibration	NIRMATA Editorial Board + Sector Working Groups	EQC Revision Bulletin
Biennial	Cross-mapping update to new framework versions	Framework Alignment Team	Updated Annex E / G links
Ad-hoc	Integration of emerging topics (AI governance, quantum security, deepfake risk)	Thematic Task Forces	Interim Addendum (Annex G-A / G-B / G-C)

All releases are version-controlled under **CC BY-SA 4.0** and published publicly for transparency and reuse.

6. Custodianship

- **Custodian:** Elytra Security — NIRMATA Programme Office
- **Change Authority:** NIRMATA Editorial Board
- **Archival Policy:** Maintain at least five years of historical EQC versions for trend analysis.
- **Public Access:** Repository maintained at [Elytra Security Public Frameworks Registry] (link to be announced).

7. Future Expansion Themes

Theme	Description
AI Risk Governance	Incorporate ISO 42001 and OECD AI Principles into Pillar 12.
Operational Technology Security	Deep-dive sub-catalogue for industrial / SCADA environments.
Cyber Insurance Readiness	Assess insurability metrics, claims traceability, and coverage controls.
Zero Trust Implementation	Evaluate ZTNA adoption across identity, network, and application tiers.
Sustainability & ESG	Link cybersecurity posture to ESG and sustainability

Controls	reporting requirements.

8. Outputs and Attachments

1. **EQC Workbook (v1.0)** — CSV format, containing the initial set of 144 core questions.
2. **EQC JSON Schema** — Machine-readable definition for portal integration.
3. **EQC Changelog** — Text summary of additions, deletions, and wording updates per release.

9. Conclusion

Annex G ensures that NIRMATA remains a **living, evidence-oriented maturity measurement system**, capable of tracking India's cybersecurity and privacy posture over time. Its modular structure, transparent governance, and trend-responsive update mechanism allow continuous improvement without disrupting backward compatibility.

By institutionalizing the Extended Question Catalogue, TRUST-IN Bharat strengthens its commitment to measurable, verifiable, and sustainable national resilience.

Custodian: Elytra Security — NIRMATA Editorial Board
License: CC BY-SA 4.0
Version: 1.0 (October 2025)

Annex G — Extended Question Catalogue (Summary)

Annex G establishes the **Extended Question Catalogue (EQC)** as the structured backbone of the NIRMATA maturity framework. It transforms the framework from a policy reference into a **quantitative, evidence-based diagnostic system**, enabling consistent benchmarking across sectors and over time. Each of the twelve NIRMATA pillars now carries 10–15 weighted questions with defined evidence types and cross-references to DPDP 2023, CERT-In 2022, ISO 27002/27701/42001, and NIST CSF 2.0. The catalogue is designed as a **living repository**, governed by the NIRMATA Editorial Board and updated through annual and biennial review cycles to reflect emerging technologies, threats, and regulatory developments. Its modular CSV/JSON structure ensures readiness for digital scoring, analytics, and national reporting. By embedding the EQC into TRUST-IN Bharat, India gains a scalable mechanism to **measure, compare, and continually strengthen** organizational resilience and information-risk maturity.

Pillar 1 — Governance & Leadership (GL)

This pillar assesses the strategic direction, accountability, and oversight structures that define how an organization governs its information security and privacy programmes.
It evaluates leadership commitment, policy governance, board involvement, resource allocation, and integration of cybersecurity within enterprise risk management.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
GL-Q01	Has the organization formally defined its information security and privacy governance structure with clear roles and reporting lines?	Org chart, policy documents, governance charter	0 = No structure 5 = Integrated CISO + DPO + Board oversight	ISO 27001 5.3 DPDP Sec 10 NIST GV 1
GL-Q02	Are board or senior leadership meetings provided with periodic cybersecurity and privacy risk updates?	Board minutes, risk dashboards, management review reports	0 = None 5 = Quarterly integrated reporting	ISO 27001 9.3 CERT-In Guideline 5 NIST GV 2
GL-Q03	Is there a formally approved enterprise information security policy reviewed at least annually?	Policy document, revision log, approval record	0 = Absent 5 = Annual board-approved policy with evidence of review	ISO 27001 5.2 DPDP Sec 9
GL-Q04	Does executive leadership allocate dedicated budget and staffing for cybersecurity and data protection initiatives?	Budget sheets, HR plans, management approvals	0 = Ad hoc 5 = Annual, risk-based allocation aligned to strategy	ISO 27001 7.2 · NIST GV 3

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
GL-Q05	Are key security and privacy roles (CISO, DPO, Risk Officer) appointed with written mandates and independence?	Appointment letters, ToRs, reporting lines	0 = Undefined 5 = Roles formally empowered and independent	DPDP Sec 10(1) · ISO 27001 5.3
GL-Q06	Are organizational objectives for information risk management defined, measurable, and aligned with corporate goals?	KRIs/KPIs, strategic plan, board presentations	0 = None 5 = Quantified KPIs linked to risk appetite	ISO 27001 6.2 · NIST GV 4
GL-Q07	Does leadership communicate a “tone at the top” emphasizing ethics, compliance, and trust in digital operations?	CEO statements, newsletters, awareness materials	0 = No messaging 5 = Visible ongoing communication culture	ISO 27001 A.5.1 · NIST GV 5
GL-Q08	Is there a defined escalation path for security, privacy, and compliance issues to reach senior management?	Escalation matrix, SOPs, org chart	0 = Undefined 5 = Formal, tested escalation workflow	CERT-In Guideline 8 · ISO 27001 A.5.25
GL-Q09	Has the organization established a governing body or committee overseeing cybersecurity and privacy programmes?	Committee charter, meeting minutes	0 = No committee 5 = Active cross-functional committee	ISO 27001 5.3 · NIST GV 6
GL-Q10	Are third-party risk and compliance updates presented to leadership periodically?	Vendor reports, audit summaries	0 = Never 5 = Quarterly integrated supply-chain risk review	ISO 27036 · DPDP Sec 8
GL-Q11	Is there a formal link between governance reporting and the organization’s internal audit or assurance function?	Internal audit plan, risk committee reports	0 = None 5 = Integrated 3-lines-of-defense model	ISO 27001 9.2 · NIST GV 7

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
GL-Q12	Does leadership participate in external benchmarking, national frameworks, or sectoral cyber maturity programmes (e.g., NIRMATA, CERT-In)?	Certificates, reports, participation records	0 = No engagement 5 = Active annual benchmarking participation	CERT-In Advisory 2022 · NIST GV 8

Scoring and Interpretation Notes — Governance & Leadership

- **Weight Distribution:** Questions GL-Q01 to GL-Q06 carry higher weights (3–5) as they represent foundational governance maturity.
- **Verification Method:** Documentary review supplemented by leadership interviews.
- **Level 4–5 Indicators:** Evidence of continuous improvement, board integration, and performance metrics tied to business outcomes.
- **Cross-Mapping:** Pillar 1 correlates strongly with ISO 27001 clauses 5 & 9 and NIST CSF Govern Function.

Pillar 2 — Risk & Compliance (RC)

This pillar evaluates the organization's capability to identify, assess, and manage cybersecurity, privacy, and operational risks in alignment with regulatory, contractual, and internal policy obligations.
It examines the maturity of risk governance, assessment processes, compliance tracking, and continuous assurance mechanisms.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
RC-Q01	Has the organization defined a formal risk management framework covering information, technology, and privacy risks?	Risk policy, framework document, board approval record	0 = None 5 = Integrated enterprise risk framework with security and privacy embedded	ISO 27005 · NIST ID.RA-1
RC-Q02	Are risk assessments conducted at planned intervals and before major system or process changes?	Risk assessment reports, change management records	0 = Ad hoc 5 = Periodic + event-driven risk assessments	ISO 27001 6.1.2 · CERT-In Guideline 3
RC-Q03	Does the risk register capture inherent, residual, and target	Risk register, mitigation plan	0 = Missing detail 5 = Dynamic register with quantified risk	ISO 27005 §8.2 · NIST ID.RA-4

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	risk levels with mitigation owners?		values and ownership	
RC-Q04	Are compliance obligations (legal, regulatory, contractual) inventoried and mapped to responsible functions?	Compliance register, legal matrix	0 = No mapping 5 = Centralized obligations inventory with ownership	DPDP Sec 11 · ISO 27001 A.5.31
RC-Q05	Is there a documented process for evaluating the impact of new or updated regulations (DPDP, CERT-In, sectoral)?	Regulatory impact assessment reports	0 = None 5 = Structured and logged with implementation tracking	DPDP Rules 2023 · NIST ID.GV-3
RC-Q06	Are data protection impact assessments (DPIAs) or privacy risk assessments performed where applicable?	DPIA reports, risk sign-offs	0 = Never 5 = Mandatory for new processing activities	DPDP Sec 10(3) · ISO 27701 §7.2.8
RC-Q07	Are audit findings and risk treatment actions tracked to closure through a centralized mechanism?	CAPA tracker, risk closure evidence	0 = Untracked 5 = Tracked with deadlines, ownership, and status metrics	ISO 27001 10.1 · NIST ID.RM-2
RC-Q08	Are risks quantitatively analyzed or prioritized based on business impact and likelihood?	Risk scoring sheets, heatmaps	0 = Qualitative only 5 = Quantitative scoring integrated with enterprise risk appetite	ISO 31000 · NIST ID.RA-5
RC-Q09	Is third-party or supplier risk formally evaluated during onboarding and periodically	Vendor risk assessments, due diligence reports	0 = None 5 = Comprehensive pre/post onboarding reviews with scoring	ISO 27036 · DPDP Sec 8(2)

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	thereafter?			
RC-Q10	Is there a compliance monitoring programme that verifies ongoing adherence to internal and external obligations?	Compliance audit plan, dashboards	0 = Ad hoc 5 = Scheduled compliance calendar with KPI tracking	ISO 27001 9.2 · NIST GV-6
RC-Q11	Does the organization maintain documented evidence of CERT-In reporting for notifiable incidents?	Incident reports, CERT-In acknowledgments	0 = None 5 = Timely submission logs with evidence of closure	CERT-In 2022 Notification §6
RC-Q12	Are residual risks accepted formally by authorized management with rationale and expiry date?	Risk acceptance forms, approval notes	0 = Informal 5 = Formal sign-off with review date	ISO 27005 §8.3 · NIST ID.RA-6

Scoring and Interpretation Notes — Risk & Compliance

- **Weight Distribution:** RC-Q01, Q02, Q03, Q04, and Q08 typically carry higher weights (3–5).
- **Verification Method:** Review of risk framework, registers, audit logs, and compliance trackers.
- **Level 4–5 Indicators:** Evidence of risk quantification, automated monitoring, and direct board reporting.
- **Cross-Mapping:** Strong correlation with ISO 27005, ISO 31000, and NIST CSF "Identify" and "Govern" functions.

Pillar 3 — Asset & Data Management (AD)

This pillar assesses the organization's ability to identify, classify, protect, and manage information assets and data throughout their lifecycle.
It emphasizes asset visibility, data inventory accuracy, ownership accountability, and lifecycle controls aligned with confidentiality, integrity, and availability requirements.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
AD-Q01	Has the organization established and maintained an up-to-date inventory of all information assets (hardware, software, data, services)?	Asset register, CMDB export, inventory policy	0 = None 5 = Automated, continuously updated inventory with ownership	ISO 27001 A.5.9 · NIST ID.AM-1
AD-Q02	Are data and assets classified based on sensitivity and business criticality (e.g., Public, Internal, Confidential)?	Data classification policy, labeling standards	0 = No classification 5 = Enterprise-wide automated classification and labeling	ISO 27001 A.5.12 · DPDP Sec 9(1)
AD-Q03	Are data owners assigned for each critical dataset or system with documented responsibilities?	Ownership matrix, policy mapping	0 = None 5 = Documented, reviewed annually	ISO 27001 A.5.9 · NIST ID.AM-6
AD-Q04	Is there an approved retention and disposal policy for data and information assets?	Data retention policy, disposal records	0 = None 5 = Enforced retention schedules with evidence of secure disposal	DPDP Sec 9(3) · ISO 27001 A.5.33
AD-Q05	Are backups conducted, encrypted, and periodically tested for data integrity and restorability?	Backup logs, test results, backup policy	0 = No backup 5 = Automated, encrypted, verified backups with test evidence	ISO 27001 A.8.13 · CERT-In Advisory §7
AD-Q06	Is there a defined process for tracking asset changes, ownership transfers, and decommissioning?	Change records, disposal logs, CMDB audit	0 = Ad hoc 5 = Integrated asset lifecycle management	ISO 27001 A.5.10 · NIST PR.AC-1
AD-Q07	Are removable media and portable devices controlled and encrypted as per policy?	Encryption logs, endpoint configuration, DLP report	0 = Uncontrolled 5 = Central policy enforcement with monitoring	ISO 27001 A.8.10 · DPDP Sec 8(4)
AD-Q08	Are personal data processing activities	ROPA (Record of Processing	0 = None 5 = Complete	DPDP Rule 5(1) · ISO

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	inventoried and linked to data subjects and purposes?	Activities), data maps	ROPA maintained and updated	27701 §7.2.4
AD-Q09	Are cloud-hosted assets inventoried with visibility into data location, ownership, and backup status?	Cloud inventory report, CSP contracts	0 = Not tracked 5 = Unified hybrid inventory integrated with CMDB	ISO 27017 §6.3.1 · NIST ID.AM-4
AD-Q10	Does the organization monitor for shadow IT and unauthorized data repositories?	CASB logs, DLP alerts, monitoring reports	0 = None 5 = Continuous detection and remediation programme	ISO 27002 8.1.2 · NIST PR.DS-3
AD-Q11	Are data integrity verification mechanisms (checksums, hashes, immutability) implemented for critical systems?	Integrity logs, WORM storage reports	0 = No control 5 = Automated integrity validation integrated with SIEM	ISO 27001 A.8.11 · CERT-In §4
AD-Q12	Is there a process to ensure data is securely transferred and logged across systems and vendors?	Secure transfer policy, encryption audit logs	0 = None 5 = Enforced encryption with audit evidence	DPDP Sec 8(3) · ISO 27033

Scoring and Interpretation Notes — Asset & Data Management

- **Weight Distribution:** AD-Q01 to AD-Q05 are foundational (weights 3–5).
- **Verification Method:** Review of inventories, data maps, retention and disposal logs, and system configurations.
- **Level 4–5 Indicators:** Continuous data inventory reconciliation, ROPA automation, cloud visibility integration.
- **Cross-Mapping:** Aligns closely with ISO 27001 Annex A.5, ISO 27701 §7.2, and NIST CSF "Identify" and "Protect" functions.

Pillar 4 — Identity & Access (IA)

This pillar evaluates how effectively an organization governs user identities, access entitlements, authentication mechanisms, and privileged account controls.
It covers access provisioning, least privilege enforcement, identity lifecycle management, and monitoring of credentials across systems and third parties.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
IA-Q01	Has the organization defined and implemented an access control policy covering all user types (employees, contractors, vendors)?	Access control policy, user onboarding SOP	0 = None 5 = Centralized and periodically reviewed access policy with full coverage	ISO 27001 A.5.15 · NIST PR.AC-1
IA-Q02	Are user accounts created, modified, and revoked through a documented and authorized workflow?	IAM system records, HR triggers, approval logs	0 = Manual 5 = Automated provisioning and deprovisioning linked to HR systems	ISO 27001 A.5.18 · CERT-In §4
IA-Q03	Are privileged accounts (admin, root, service) inventoried and reviewed periodically?	Privileged account list, PAM logs	0 = Unknown 5 = Managed via PAM with quarterly certification	ISO 27001 A.5.19 · NIST PR.AC-4
IA-Q04	Is multifactor authentication (MFA) enforced for remote access and sensitive systems?	Authentication policy, system configs, MFA logs	0 = None 5 = Enforced for all high-risk users and critical systems	CERT-In Directive 2022 §5 · NIST PR.AC-7
IA-Q05	Are access rights reviewed at defined intervals and upon job change or termination?	Access review reports, HR termination checklist	0 = Never 5 = Automated quarterly access reviews with sign-off	ISO 27001 A.5.20 · DPDP Sec 8(4)
IA-Q06	Is the principle of least privilege applied to all systems and applications?	Role matrix, policy mapping, system configs	0 = Ad hoc 5 = Enforced via role-based access control (RBAC)	ISO 27001 A.5.17 · NIST PR.AC-6
IA-Q07	Are shared accounts prohibited or technically restricted?	Account policy, logs, enforcement reports	0 = Allowed 5 = Prohibited and enforced via system controls	ISO 27001 A.5.21 · CERT-In §3
IA-Q08	Are dormant or inactive accounts automatically disabled or deleted after a defined period?	IAM logs, system reports	0 = Never 5 = Automated deactivation based	ISO 27001 A.5.22 · NIST PR.AC-3

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
			on policy	
IA-Q09	Are service accounts assigned to specific owners and credentials rotated regularly?	Ownership records, rotation logs	0 = No ownership 5 = Automated rotation and ownership traceability	ISO 27001 A.5.19 · NIST PR.AC-4
IA-Q10	Is there centralized identity federation or SSO implemented for enterprise applications?	SSO config, federation diagram	0 = None 5 = Fully federated identity system integrated with MFA	ISO 27033 · NIST PR.AC-1
IA-Q11	Are access logs for privileged actions retained and reviewed for anomalies?	SIEM reports, PAM session logs	0 = Not logged 5 = Continuous monitoring with alerting	ISO 27001 A.8.15 · CERT-In §6
IA-Q12	Are third-party and vendor access accounts governed through time-bound approval and monitoring?	Vendor access logs, contract clauses	0 = Open access 5 = Controlled through JIT access with audit trail	ISO 27036 §7.3 · DPDP Sec 8(2)

Scoring and Interpretation Notes — Identity & Access

- **Weight Distribution:** IA-Q02, Q03, Q04, Q05, and Q06 hold higher weights (3–5).
- **Verification Method:** Review IAM configurations, HR triggers, PAM evidence, and access reviews.
- **Level 4–5 Indicators:** Centralized identity governance, automated recertification, adaptive authentication.
- **Cross-Mapping:** Aligns with ISO 27001 Annex A.5.15–A.5.22 and NIST CSF "Protect – Access Control" category.

Pillar 5 — Infrastructure Security (IS)

This pillar examines the organization's ability to secure its IT and OT infrastructure, including servers, endpoints, network devices, and cloud resources.
It evaluates configuration management, patching, hardening, vulnerability management, and network segmentation practices.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
IS-Q01	Has the organization implemented a documented and approved baseline configuration standard for all	Hardening guides, baselines, policy	0 = None 5 = Baselines approved,	ISO 27001 A.8.9 · NIST PR.IP-1

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	systems?	documents	enforced, and verified through automation	
IS-Q02	Are operating systems and software kept current through a formal patch management process?	Patch reports, WSUS logs, change tickets	0 = Ad hoc 5 = Automated patch deployment with exception tracking	ISO 27001 A.8.8 · CERT-In §7
IS-Q03	Is network segmentation implemented between IT, OT, and management zones?	Network diagrams, firewall configs, VLAN plans	0 = Flat network 5 = Segmented with defined trust boundaries	ISO 27033 §7 · NIST PR.AC-5
IS-Q04	Are endpoint protection and EDR tools deployed and monitored across all systems?	EDR console report, coverage metrics	0 = None 5 = 100% coverage with alert correlation	ISO 27001 A.8.15 · CERT-In §5
IS-Q05	Is vulnerability scanning conducted periodically, and are findings remediated based on risk?	Scan reports, remediation logs	0 = None 5 = Continuous scanning integrated into CI/CD pipeline	ISO 27001 A.5.23 · NIST DE.CM-8
IS-Q06	Are firewall and network device configurations reviewed and approved periodically?	Review logs, change control tickets	0 = Never 5 = Quarterly review with formal sign-off	ISO 27033 §8.2 · CERT-In §4
IS-Q07	Are administrative interfaces and remote management ports protected through MFA, VPN, or network isolation?	Network configs, access logs	0 = Open access 5 = Restricted and monitored via secure channels	ISO 27033 §9.3 · NIST PR.AC-7
IS-Q08	Is there an intrusion detection/prevention or network monitoring solution in place?	IDS/IPS logs, SOC reports	0 = None 5 = Monitored continuously with correlation to SIEM	ISO 27001 A.8.16 · NIST DE.CM-1
IS-Q09	Are configurations of critical infrastructure (e.g., servers, routers, controllers) backed	Backup configs, version	0 = None 5 = Versioned, immutable	ISO 27001 A.8.12 · CERT-In §6

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	up and protected from tampering?	control, access logs	backups of configs	
IS-Q10	Are unauthorized devices detected and blocked on internal networks?	NAC logs, asset discovery reports	0 = Unchecked 5 = NAC enforced with automatic quarantine	ISO 27001 A.5.10 · NIST PR.AC-1
IS-Q11	Are wireless networks secured through authentication, encryption, and segmentation from core infrastructure?	WLAN policy, config snapshots	0 = Open access 5 = WPA3/802.1X implemented with monitoring	ISO 27033 §10 · NIST PR.AC-5
IS-Q12	Are OT and IoT systems inventoried and governed by equivalent cybersecurity controls?	OT asset list, hardening policy	0 = Not covered 5 = Integrated into enterprise security management	ISO 62443 · NIST ID.AM-2

Scoring and Interpretation Notes — Infrastructure Security

- **Weight Distribution:** IS-Q01, Q02, Q04, Q05, and Q08 are core controls (weights 3–5).
- **Verification Method:** Review configuration baselines, scan logs, SOC reports, and firewall rule reviews.
- **Level 4–5 Indicators:** Continuous vulnerability management, automated patching, integrated OT security visibility.
- **Cross-Mapping:** Corresponds to ISO 27001 Annex A.8, ISO 27033, NIST CSF "Protect" and "Detect," and CERT-In operational guidelines.

Pillar 6 — Application & Product Security (AP)

This pillar evaluates how securely software is planned, designed, built, tested, released, and maintained across the SDLC, including first-party code, third-party components, APIs, infrastructure as code, and CI/CD pipelines.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
AP-Q01	Is a secure SDLC policy defined and enforced for all products and internal apps?	Secure SDLC policy, stage gates, audit logs	0 = None 5 = Mandatory stage gates with metrics and enforcement	ISO 27034 · ISO 27001 A.8.28 · NIST PR.IP-3
AP-	Are developers trained annually on secure	Training records, quiz scores,	0 = Ad hoc	ISO 27001 A.6.3 · OWASP

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
Q02	coding and common weakness classes?	curriculum	5 = Role-based annual training with effectiveness tracking	SAMM EDU
AP-Q03	Is threat modeling performed for high-risk systems and significant changes?	Data flow diagrams, STRIDE documents	0 = Never 5 = Required for epics and major releases with review	ISO 27034 §7 · NIST PR.IP-12
AP-Q04	Are SAST and secret scanning integrated into the CI pipeline with break-the-build rules?	CI configs, scan reports, PR checks	0 = Manual 5 = Automated on every commit with policy gating	OWASP ASVS 1.14 · ISO 27001 A.8.29
AP-Q05	Are DAST/IAST tests executed for web and API surfaces prior to release?	DAST reports, IAST findings, tickets	0 = None 5 = Automated pre-release with tracked remediation SLAs	OWASP ASVS 14.x · NIST DE.CM-8
AP-Q06	Is a Software Bill of Materials (SBOM) generated and third-party components vetted for vulnerabilities and licenses?	SBOM files, SCA reports, license policy	0 = None 5 = SBOM per build with continuous SCA and license gating	ISO 5230 (OpenChain) · NIST SSDF PS.3.2
AP-Q07	Are APIs inventoried, authenticated, rate-limited, and tested for common API flaws?	API gateway configs, test suites, inventory	0 = Unknown 5 = Central API management with automated testing	OWASP API Security Top 10 · ISO 27033 §9
AP-Q08	Are IaC templates scanned and environments protected with policy-as-code before provisioning?	IaC repos, policy-as-code results	0 = Not scanned 5 = Mandatory scan and enforcement in CI/CD	NIST SP 800-53 CM-2 · CIS Benchmarks
AP-Q09	Are builds reproducible, artifacts signed, and releases tracked with provenance?	Sigstore/cosign logs, SLSA level doc	0 = Unsigned 5 = Provenance attestations with signing and verification	SLSA v1 · NIST SSDF PW.4.1

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
AP-Q10	Is there a coordinated disclosure and bug bounty or vulnerability intake process?	Policy page, intake tickets, SLA metrics	0 = None 5 = Public intake with triage, SLAs, and reporting	ISO 29147 · ISO 30111
AP-Q11	Are privacy-by-design checks embedded into design and pre-release reviews?	DPIA checklists, design review templates	0 = Not considered 5 = Mandatory PB&D checklist aligned to DPDP	ISO 27701 §7.3 · DPDP Rules
AP-Q12	Are production security incidents tied back into backlog with root cause and control improvements?	Postmortems, CAPA items, sprint links	0 = Informal 5 = Systematic RCAs feeding SDLC improvements	ISO 27001 10.2 · NIST RC.IM-1

Scoring and Interpretation Notes — Application & Product Security

- **Weight priorities:** AP-Q01, Q03, Q04, Q06, Q09 are typically weight 4–5 due to systemic risk reduction and supply chain assurance.
- **Verification method:** Review CI/CD configs, scan outputs, SBOMs, signed artifact logs, change records, and ticketing workflow.
- **Level 4–5 indicators:** Policy-gated pipelines, automated testing coverage, signed provenance, continuous SCA, measurable MTTR on code defects.
- **Cross-mapping:** OWASP ASVS and SAMM, NIST SSDF, ISO 27034, ISO 27701, SLSA supply chain levels.

Pillar 7 — Monitoring & Detection (MD)

This pillar assesses the organization's ability to detect security events, anomalies, and policy violations across networks, systems, and applications.
It evaluates logging coverage, telemetry quality, correlation, alerting, and the maturity of security operations and analytics.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
MD-Q01	Has the organization defined a centralized logging and monitoring policy specifying scope, retention, and responsibilities?	Logging policy, SIEM SOPs	0 = None 5 = Enterprise-wide policy with automated enforcement	ISO 27001 A.8.15 · NIST DE.CM-7
MD-Q02	Are critical systems, applications, and network	SIEM config, log source list	0 = Partial 5 = 100% coverage	ISO 27001 A.8.16 · CERT-

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	devices sending logs to a centralized SIEM or log analytics platform?		of all critical assets	In §6
MD-Q03	Are logs correlated and analyzed to detect anomalies, attacks, and policy violations?	SIEM correlation rules, detection dashboards	0 = No correlation 5 = Correlation and ML-based anomaly detection active	NIST DE.CM-1 · MITRE ATT&CK
MD-Q04	Are alerts triaged and prioritized based on severity, impact, and context?	SOC playbooks, triage logs	0 = Manual 5 = Automated prioritization with enrichment	ISO 27035-1 §7 · NIST DE.CM-4
MD-Q05	Is there a documented process for tuning detection rules and reducing false positives?	Rule tuning logs, change records	0 = None 5 = Continuous tuning and validation cycle	ISO 27001 10.2 · NIST DE.CM-6
MD-Q06	Are endpoint and network telemetry integrated to enable unified visibility?	SIEM topology, integration diagrams	0 = Siloed 5 = Unified telemetry with correlation and cross-source alerts	NIST DE.CM-7 · CERT-In §5
MD-Q07	Are alerts and security events tracked to closure with metrics (MTTD, MTTR)?	SOC reports, ticket metrics	0 = Not tracked 5 = Metrics dashboard reviewed monthly	ISO 27035-2 §8 · NIST DE.CM-3
MD-Q08	Are external threat intelligence feeds used to enrich detections and correlate with observed activity?	TI integration logs, feed list	0 = None 5 = Automated integration and enrichment	ISO 27002 8.16 · NIST DE.CM-2
MD-Q09	Is monitoring extended to cloud workloads, containers, and SaaS services?	Cloud SIEM configs, CSPM dashboards	0 = No visibility 5 = Integrated cloud-native logging into SIEM	ISO 27017 §12.4.1 · NIST DE.CM-8
MD-Q10	Are time synchronization controls (NTP, chrony) enforced across systems to ensure accurate	System configs, NTP logs	0 = Unmanaged 5 = Centralized, enforced synchronization	ISO 27001 A.8.14 · CERT-In §4

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	logging?			
MD-Q11	Are insider threat or behavioral analytics tools in use to detect anomalous user actions?	UEBA reports, detection policy	0 = None 5 = Automated UEBA integrated with HR triggers	NIST DE.CM-7 · DPDP Sec 10(4)
MD-Q12	Are monitoring systems themselves protected and periodically audited for tamper-resistance?	Access control lists, audit logs	0 = Unprotected 5 = Segregated, monitored, and integrity-checked	ISO 27001 A.8.11 · CERT-In §3

Scoring and Interpretation Notes — Monitoring & Detection

- **Weight Distribution:** MD-Q02, Q03, Q04, Q06, and Q08 typically weight 4–5 due to operational criticality.
- **Verification Method:** Review SIEM configurations, dashboards, incident tickets, threat intel integrations.
- **Level 4–5 Indicators:** Correlated, enriched detections; automated triage; integration with incident response workflows.
- **Cross-Mapping:** ISO 27035, ISO 27001 A.8.15–A.8.16, NIST CSF "Detect" function, MITRE ATT&CK operational coverage.

Pillar 8 — Incident Readiness (IR)

This pillar evaluates preparedness to detect, respond to, communicate, and recover from security and privacy incidents.
It covers governance of incident response, playbooks, drills, tooling, legal/CERT-In obligations, communications, and continual improvement.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
IR-Q01	Is there a formally approved Incident Response Plan (IRP) defining roles, phases, and activation criteria?	IRP document, RACI, approval logs	0 = None 5 = Enterprise IRP with annual approval and distribution	ISO 27035-1 §7 · ISO 27001 6.1
IR-Q02	Are incident categories, severities, and SLAs defined and used consistently across teams?	Severity matrix, SLA policy, ticket fields	0 = Undefined 5 = Standardized taxonomy with tooling enforcement	ISO 27035-1 §8 · NIST RS.MI-1
IR-Q03	Are playbooks/runbooks maintained for top attack scenarios (e.g.,	Playbook library, version history	0 = None 5 = Scenario	ISO 27035-1 §8.3 · MITRE

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	ransomware, BEC, data breach, OT outage)?		playbooks tested and updated post-incident	
IR-Q04	Are incident roles staffed and trained (IR lead, comms, legal, forensics, business owner)?	Training records, role assignments	0 = Ad hoc 5 = Role-based training with periodic refreshers	ISO 27001 7.2 · NIST RS.IM-1
IR-Q05	Are detection-to-response handoffs defined between SOC and IR teams with measurable MTTD/MTTR?	Handoff SOP, metrics dashboard	0 = Informal 5 = Measured, automated handoffs with targets	NIST DE.RP-1 · RS.AN-1
IR-Q06	Are mock exercises/tabletops conducted at least annually, with post-exercise improvements tracked?	Exercise reports, CAPA tracker	0 = None 5 = Annual+ exercises; actions tracked to closure	ISO 27035-3 §6 · NIST RS.IM-2
IR-Q07	Is digital forensics capability available (internal or retainer) with chain-of-custody procedures?	Forensics SOP, retainer contract, forms	0 = None 5 = Retained capability with trained staff and tools	ISO 27037 · ISO 27035-2
IR-Q08	Are CERT-In reporting obligations integrated (where applicable) with timelines and evidence of submission?	CERT-In reports, acknowledgments	0 = Not addressed 5 = Timely submissions with audit trail	CERT-In 2022 §6
IR-Q09	Is breach response integrated with privacy requirements (DPDP) including notification criteria and timelines?	DPIA addenda, notification templates	0 = Not defined 5 = DPDP-ready process with counsel review	DPDP Act 2023 · ISO 27701 §7.4
IR-Q10	Is there a communications plan for incidents (internal, customer, regulator, media) with approved	Comms playbook, templates, approvals	0 = None 5 = Pre-approved messaging aligned to legal/compliance	ISO 27035-1 §8.4

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	templates?			
IR-Q11	Are backups, recovery steps, and isolation strategies integrated into response for destructive attacks?	Recovery runbooks, DR drills	0 = Separate 5 = IR and DR integrated; recovery tested	ISO 27031 · NIST RS.RP-1
IR-Q12	Are incident learnings fed into control improvements, training, and threat models (closed-loop)?	Postmortems, backlog links, metrics	0 = Untracked 5 = Systematic RCAs with measurable reduction in repeat issues	ISO 27001 10.2 · NIST RC.IM-1

Scoring and Interpretation Notes — Incident Readiness

- **Weight priorities:** IR-Q01, Q02, Q03, Q06, Q08, Q11 typically weight 4–5 due to legal and operational criticality.
- **Verification method:** Review IRP, playbooks, training records, drill reports, CERT-In submissions, postmortems, and metrics.
- **Level 4–5 indicators:** Tested scenario playbooks, measured MTTD/MTTR, regulator-ready reporting, integrated DR, and continuous improvement loop.
- **Cross-mapping:** ISO 27035 (parts 1–3), ISO 27031, ISO 27701 breach handling, NIST CSF "Respond/Recover," CERT-In 2022 notifications.

Pillar 9 — Business Continuity & Resilience (BR)

This pillar evaluates the organization's ability to sustain critical operations during and after disruptive incidents.
It examines business impact analysis, continuity planning, disaster recovery, redundancy, and crisis management integration.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
BR-Q01	Has the organization conducted a formal Business Impact Analysis (BIA) identifying critical functions, RTOs, and RPOs?	BIA report, RTO/RPO matrix	0 = None 5 = Enterprise-wide BIA reviewed annually	ISO 22301 §8.2 · ISO 27031 §7.3
BR-Q02	Is there a documented Business Continuity Plan (BCP) aligned to the BIA and updated at least	BCP document, revision history	0 = None 5 = BCP integrated with IR and DR plans; annual	ISO 22301 §8.3 · ISO 27031

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	annually?		review	
BR-Q03	Are Disaster Recovery (DR) strategies defined and tested for critical systems and infrastructure?	DR plan, test results, failover reports	0 = None 5 = Periodic full failover and recovery testing	ISO 27031 §8.4 · NIST CP-9
BR-Q04	Are backup facilities (data centers, cloud, or alternate sites) validated for readiness and capacity?	DR site audit reports, vendor SLAs	0 = None 5 = Validated alternate sites with recent test evidence	ISO 22301 §8.4.4 · CERT-In §7
BR-Q05	Are continuity roles, teams, and escalation paths clearly defined and trained?	Org chart, training logs, contact rosters	0 = Unclear 5 = Defined teams with tested response readiness	ISO 22301 §8.3.2 · NIST CP-1
BR-Q06	Are periodic BCP and DR drills conducted and results analyzed for improvements?	Drill reports, CAPA logs	0 = None 5 = Annual+ exercises with measurable improvement metrics	ISO 22301 §9.1 · NIST CP-4
BR-Q07	Is resilience embedded in system design (redundancy, fault tolerance, high availability)?	Architecture diagrams, uptime reports	0 = Not considered 5 = Designed and validated fault-tolerant systems	ISO 27001 A.8.13 · NIST PR.IP-9
BR-Q08	Are dependencies on third parties or supply-chain partners addressed in continuity plans?	BCP annex, vendor contracts	0 = Ignored 5 = Mapped and contractually obligated	ISO 22301 §8.3.5 · ISO 27036
BR-Q09	Is cyber resilience integrated with business continuity metrics (e.g., cyber RTO, data immutability)?	Cyber resilience plan, recovery logs	0 = None 5 = Combined metrics tracked across business and IT	ISO 27031 §8.6 · NIST RC.RP-1
BR-Q10	Does leadership review continuity and recovery performance at least	Management review minutes, KPI dashboards	0 = Never 5 = Formal review with improvement	ISO 22301 §9.3 · ISO 27001 9.3

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	annually?		decisions	

Scoring and Interpretation Notes — Business Continuity & Resilience

- **Weight priorities:** BR-Q01, Q02, Q03, and Q09 hold weight 4–5; others typically 2–3.
- **Verification method:** Review BIAs, BCPs, DR plans, test reports, and management reviews.
- **Level 4–5 indicators:** Cross-functional continuity governance, integrated IR/DR, automated failover, and supplier continuity evidence.
- **Cross-mapping:** ISO 22301, ISO 27031, ISO 27001 A.8.13, NIST CSF "Recover" function, CERT-In §7 continuity expectations.

Pillar 10 — Privacy & Data Protection (PD)

This pillar evaluates how well the organization protects personal data across its lifecycle in line with the DPDP Act 2023 and aligned international standards.
It covers governance, lawful basis, consent and notices, data subject rights, DPIA, vendor management, breach handling, and transparency.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
PD-Q01	Is there a formally approved privacy governance model with named Data Fiduciary leadership (e.g., DPO/Privacy Lead), roles, and accountability?	Org chart, appointment letter, governance charter	0 = None 5 = Board-recognized role with mandate, KPIs, and independence	DPDP Sec 10; ISO 27701 §5.2; ISO 27001 5.3
PD-Q02	Are privacy notices accurate, comprehensive, and context-specific, and are they version-controlled and easily accessible?	Privacy policy, layered notices, change logs	0 = Generic/dated 5 = Contextual, layered, multilingual with version history	DPDP Sec 5; ISO 27701 §7.3.2
PD-Q03	Is the lawful basis recorded for each processing purpose (consent or permitted uses), with evidence of purpose limitation?	Lawful-basis register, purpose mapping	0 = Not recorded 5 = Mapped per purpose with audit trail	DPDP Sec 4–7; ISO 27701 §7.2.1
PD-Q04	Is consent captured, granular, revocable, and demonstrable, with logs of	Consent logs, UI screenshots, revocation	0 = Ad hoc 5 = System-enforced consent	DPDP Sec 6; ISO 27701 §7.3.3

	obtain/withdraw actions?	workflow	lifecycle with proofs	
PD-Q05	Are data principal (DSAR) requests supported end-to-end (access, correction, erasure, grievance) with SLAs and identity verification?	DSAR tracker, SOPs, response templates	0 = Informal 5 = SLA-driven DSAR process with metrics and audits	DPDP Sec 11–12; ISO 27701 §7.3.5
PD-Q06	Is a record of processing activities (ROPA) maintained, including categories, retention, processors, and security measures?	ROPA export, data maps, inventories	0 = None 5 = System-generated ROPA with periodic attestation	ISO 27701 §7.2.4; ISO 27001 A.5.9
PD-Q07	Are DPIAs or risk assessments performed for high-risk processing, novel tech, large-scale profiling, or mandated scenarios?	DPIA reports, sign-offs, mitigations	0 = Not practiced 5 = Mandatory triggers with review cadence	DPDP Sec 10(3); ISO 27701 §7.2.8
PD-Q08	Are retention schedules defined and enforced with secure deletion/archiving based on purpose completion?	Retention policy, purge logs, WORM/archive evidence	0 = Undefined 5 = Automated retention and defensible deletion	DPDP Sec 9(3); ISO 27701 §7.2.3; ISO 27001 A.5.33
PD-Q09	Are processor (vendor) contracts governed with privacy and security clauses, audits, incident duties, and sub-processor controls?	DPAs, SCCs/clauses, audit reports	0 = Boilerplate 5 = Standardized DPA with ongoing assurance and right-to-audit	DPDP Sec 8(2); ISO 27701 §6.2.1; ISO 27036
PD-Q10	Are cross-border transfers governed by policy aligned with Government notifications, including risk assessment and record-keeping?	Transfer policy, country lists, TRA reports	0 = Unmanaged 5 = Policy-driven with approvals and evidence logs	DPDP Sec 16 (as notified); ISO 27701 §6.13
PD-Q11	Are privacy breaches reported and managed per law, including timely notification to the Data Protection Board of India	Incident logs, notification templates, submissions	0 = Undefined 5 = Integrated IR + legal workflow with timelines	DPDP Sec 8(5) & breach rules; CERT-In 2022 §6; ISO 27701

	and affected individuals where required?		and proofs	§7.4
PD-Q12	Are children's data and high-risk categories treated with enhanced safeguards (age gating, verifiable consent, profiling limits)?	Age-verification design, parental consent records	0 = Not addressed 5 = Enforced controls with periodic effectiveness checks	DPDP Sec 9; ISO 27701 §7.3.8

Scoring and Interpretation Notes — Privacy & Data Protection

- **Weight priorities:** PD-Q03 (lawful basis), PD-Q04 (consent lifecycle), PD-Q05 (DSAR), PD-Q07 (DPIA), PD-Q11 (breach) typically weight 4–5 due to legal exposure.
- **Verification method:** Review lawful-basis/ROPA registers, DSAR tracker, consent logs, DPIAs, DPAs, breach evidence, and retention enforcement artifacts.
- **Level 4–5 indicators:** Systemized, auditable records; automated consent/retention; regulator-ready breach workflow; continuous vendor assurance.
- **Cross-mapping:** DPDP Act 2023 core duties of Data Fiduciaries, ISO 27701 operational controls, ISO 27001 Annex A governance and technical safeguards, CERT-In breach reporting for security incidents.

Pillar 11 — Supply-Chain Security (SC)

This pillar evaluates the organization's ability to manage cybersecurity and privacy risks arising from suppliers, contractors, service providers, and technology partners.
It focuses on due diligence, onboarding, contractual controls, monitoring, incident response, and continuous assurance mechanisms.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
SC-Q01	Is there a defined third-party risk management policy outlining supplier selection, classification, and assessment processes?	TPRM policy, classification matrix	0 = None 5 = Policy-driven, risk-based supplier lifecycle	ISO 27036-1 §6 · NIST ID.SC-1
SC-Q02	Are pre-contract due diligence and security/privacy evaluations conducted for vendors handling critical data or	Due diligence checklist, reports	0 = None 5 = Mandatory pre-onboarding assessment and scoring	ISO 27036-2 §7.2 · DPDP Sec 8(2)

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	systems?			
SC-Q03	Do supplier contracts include data protection clauses, confidentiality, breach reporting, and right-to-audit provisions?	Signed contracts, sample clauses	0 = Absent 5 = Standard DPA and cyber clauses in all agreements	DPDP Sec 8(2) · ISO 27036-3 §8
SC-Q04	Are vendors classified based on criticality (high, medium, low) and reassessed periodically?	Vendor risk register, scoring matrix	0 = Not classified 5 = Periodic risk review and reclassification	ISO 27036-2 §7.3 · NIST ID.SC-2
SC-Q05	Are suppliers required to provide certifications or assurance (ISO 27001, SOC 2, etc.) or undergo audits?	Certificates, audit reports	0 = None 5 = Assurance evidence mandated and tracked	ISO 27036-3 §8.5 · NIST ID.SC-3
SC-Q06	Is there a formal onboarding and offboarding process for suppliers, including access removal and data return?	Onboarding/offboarding logs, SOPs	0 = Informal 5 = Automated, tracked supplier lifecycle management	ISO 27001 A.5.21 · NIST PR.AC-1
SC-Q07	Are suppliers monitored for cybersecurity performance and incidents during the contract term?	Scorecards, reports, SOC alerts	0 = None 5 = Continuous monitoring with defined thresholds	ISO 27036-3 §8.6 · CERT-In §4
SC-Q08	Are subcontractors or sub-processors identified and subject to equivalent controls and contractual	Sub-processor lists, contracts	0 = Untracked 5 = Fully documented and bound under same clauses	DPDP Sec 8(2)(c) · ISO 27701 §6.2.2

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	obligations?			
SC-Q09	Are supply-chain cybersecurity incidents reportable within defined timelines, and is the escalation process tested?	Incident logs, notification templates	0 = No requirement 5 = Defined, contractually enforced reporting	CERT-In §6 · ISO 27036-3 §8.8
SC-Q10	Are third-party tools and open-source components vetted for vulnerabilities and licensing before integration?	SCA reports, OSS policy	0 = Never 5 = Automated scanning in CI/CD and procurement vetting	ISO 5230 · NIST SSDF PS.3.2
SC-Q11	Is there a centralized repository or register of all active suppliers with associated risk ratings and review dates?	TPRM register, dashboards	0 = None 5 = Centralized, automated risk register integrated with procurement	ISO 27036-1 §7.3 · NIST ID.SC-4
SC-Q12	Are suppliers included in continuity or incident response drills for integrated resilience?	Joint drill reports, meeting minutes	0 = Never 5 = Periodic participation and feedback cycle	ISO 22301 §8.3.5 · ISO 27035-3

Scoring and Interpretation Notes — Supply-Chain Security

- **Weight priorities:** SC-Q02, Q03, Q05, Q07, and Q09 typically weight 4–5 due to systemic dependency risk.
- **Verification method:** Review vendor registers, contracts, due diligence templates, audit evidence, and monitoring dashboards.
- **Level 4–5 indicators:** Continuous assurance platform, joint exercises, contractual escalation, third-party telemetry feeds.
- **Cross-mapping:** ISO 27036 series, ISO 27701 processor controls, NIST CSF "Identify – Supply Chain" and "Protect – Third Party," CERT-In contractual reporting duties.

Pillar 12 — Culture, Training & Awareness (CT)

This pillar evaluates whether people, behaviors, and organizational culture actively support secure and privacy-respecting operations.

It covers leadership tone, policy understanding, role-based training, secure behaviors, simulated exercises, and continuous measurement.

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
CT-Q01	Is there a documented awareness strategy and annual plan aligned to risk, incidents, and regulatory priorities?	Awareness strategy, calendar, comms plan	0 = None 5 = Risk-based annual plan with KPIs and budget	ISO 27001 A.6.3 · NIST PR.AT-1
CT-Q02	Do all employees complete mandatory induction and annual refresher training on security and privacy?	LMS reports, completion dashboards	0 = Ad hoc 5 = ≥98% completion with tracked exceptions	ISO 27001 7.2 · NIST PR.AT-2
CT-Q03	Is training role-based (e.g., developers, admins, legal, support, OT operators, executives)?	Role curricula, mapping matrix	0 = Generic only 5 = Role-specific paths with assessments	ISO 27002 6.3.2 · NIST PR.AT-3
CT-Q04	Are developers trained on secure coding, OWASP Top 10/API, supply-chain hygiene, and privacy-by-design?	Course records, quiz scores	0 = None 5 = Annual + just-in-time modules tied to SDLC gates	ISO 27034 · NIST SSDF GOV.2
CT-Q05	Are phishing/social engineering simulations conducted with targeted coaching for at-risk users?	Simulation reports, coaching logs	0 = Never 5 = Quarterly sims with trending fail-rate reduction	ISO 27002 5.10 · NIST PR.AT-5
CT-Q06	Do personnel attest to understanding policies (AUP, IR, privacy notices) at least annually?	Attestation records, e-sign logs	0 = No attestation 5 = Annual e-attestations with tracking	ISO 27001 5.2/7.3 · DPDP Sec 6
CT-Q07	Is there an anonymous reporting channel (hotline/portal) for security or privacy concerns, with non-retaliation policy?	Hotline URL, case logs, policy excerpt	0 = None 5 = Active channel with SLAs and governance	ISO 37301 §8.9 · ISO 27001 A.5.1
CT-Q08	Are leaders visibly engaged (messages,	CEO memos, town-hall decks	0 = Absent 5 = Quarterly	ISO 27001 5.1 · NIST GV

ID	Question	Evidence Examples	Maturity Scale (0–5 Summary)	Control References
	town-halls, metrics reviews) to reinforce "tone at the top"?		leadership comms with KPI review	
CT-Q09	Are third-party staff and contractors included in training and policy attestation where they access systems/data?	Contract clauses, LMS invites	0 = Excluded 5 = Contractually required, tracked in LMS	ISO 27036 · DPDP Sec 8(2)
CT-Q10	Are culture and behavior measured (surveys, spot checks, secure-behavior metrics) and actions taken on results?	Survey results, action plans	0 = Not measured 5 = Biannual survey with improvement initiatives	ISO 27001 9.1 · NIST MEA
CT-Q11	Are real incidents and near-misses converted into learning content (micro-lessons, safety moments)?	Postmortems, micro-learning	0 = No feedback loop 5 = Continuous learning tied to events	ISO 27035-3 §6 · ISO 27001 10.2
CT-Q12	Are training effectiveness and behavior change evaluated (beyond completion) using defined models (e.g., Kirkpatrick)?	Evaluation rubric, outcome metrics	0 = Completion only 5 = Level 3–4 outcomes (behavior/results) tracked	ISO 30414 L&D · NIST PR.AT

Scoring and Interpretation Notes — Culture, Training & Awareness

- **Weight priorities:** CT-Q02 (coverage), CT-Q03 (role-based), CT-Q05 (phishing/SE), CT-Q10 (measurement), CT-Q12 (effectiveness) typically weight 4–5.
- **Verification method:** Review LMS exports, curricula, simulation reports, attestation records, leadership comms, survey outcomes, and improvement logs.
- **Level 4–5 indicators:** Risk-aligned plan, role-specific pathways, measurable reduction in risky behaviors, executive sponsorship, and outcome-based evaluation.
- **Cross-mapping:** ISO/IEC 27001 clauses 5, 7, 9, 10; ISO/IEC 27002 section 6.3; NIST CSF "Protect—Awareness & Training (PR.AT)"; DPDP duties for personnel handling personal data.

4A. Pillar Scoring Guidance

This section defines the standardized method for calculating maturity scores for each NIRMATA pillar based on the Extended Question Catalogue (EQC).
It ensures consistency, comparability, and auditability across organizations, sectors, and assessment cycles.

Alignment Note — Consistency with Section 6: Scoring and Interpretation Framework

This scoring methodology is fully harmonized with the **NIRMATA Scoring and Interpretation Framework** described in Section 6 of the whitepaper.

In this Annex, the term *"pillar"* is equivalent to *"domain"* used in Section 6.

Both sections apply the same arithmetic sequence—weighted averaging of question scores, normalization of results to a 0–100 range, and conversion to a 0–5 maturity level.

Evidence Confidence Factors (ECF) and sector-specific weighting coefficients are applied identically in both formulations. The mathematical relationship between the two presentations is as follows

Composite Maturity Index (0–5 scale) = (Σ Weighted Percentages ÷ 100) × 5

Thus, whether expressed in percentage form (Annex G) or in weighted domain contributions (Section 6), the computed maturity levels are equivalent. This clarification ensures methodological consistency and prevents any ambiguity when interpreting or comparing results across assessments.

1. Scoring Scale

Each question in the EQC is rated on the **0–5 maturity scale** defined in Annex A:

Score	Descriptor	Interpretation
0	**Absent**	Control not implemented or unknown.
1	**Initial**	Ad hoc, reactive, dependent on individuals.
2	**Defined**	Policy or process exists but inconsistently applied.
3	**Implemented**	Consistently executed and documented.
4	**Measured**	Monitored for performance and effectiveness.
5	**Optimized**	Continually improved and integrated enterprise-wide.

2. Weighting Factors

Each question carries a **weight** between 1 and 5 in the EQC dataset.
Weights reflect relative importance, legal/regulatory impact, and control criticality.

Weight	Typical Meaning
1	Supporting or contextual control
2	Process-level control
3	Foundational requirement
4	High-impact safeguard
5	Critical / legally mandated control

Weights may differ across pillars (e.g., governance questions generally heavier than cultural ones).

3. Pillar Score Calculation

Weighted Average Score (for a given pillar p) =

$$(\Sigma(Ri,p \times Wi,p)) \div (\Sigma Wi,p)$$

Where:
$R_{i,p}$ = Response score for question i in pillar p (0–5 scale)
$W_{i,p}$ = Weight assigned to question i in pillar p (1–5)
Σ = Sum over all questions in that pillar (n questions)

The result is rounded to one decimal (e.g., 3.7) and mapped to the nearest whole-level maturity band (0–5) for reporting.

4. Normalization Across Pillars

Because pillars contain different total weights, scores are normalized to ensure equitable contribution to the overall NIRMATA maturity index:

Normalized Pillar Score (for pillar p) = (Weighted Average Score for pillar p ÷ 5) × 100

All twelve normalized pillar scores are then combined to form the **Composite Maturity Index (CMI)** as follows:

$$CMI = (\Sigma(\text{Normalized Pillar Score}_p \times Pw)) \div (\Sigma Pw)$$

Where:

- Normalized Pillar Score$_p$ = normalized score for each pillar *p*
- Pw = pillar-level importance coefficient (default value = 1)
- Σ = summation across all twelve pillars

The resulting CMI represents the organization's **overall maturity** on a 0–100 scale, which is then mapped back to a **0–5 maturity level** for reporting and visualization.

5. Interpretation Bands

Average (0–5)	Normalized (%)	Maturity Level	Interpretation
0.0–1.0	0–20	**Initial**	Ad hoc, limited awareness.
1.1–2.0	21–40	**Developing**	Basic structure emerging.
2.1–3.0	41–60	**Defined**	Documented and repeatable.
3.1–4.0	61–80	**Managed**	Monitored and measured.
4.1–5.0	81–100	**Optimized**	Continually improved, benchmarked.

6. Verification and Confidence Grading

Assessors record evidence per question and assign an Evidence Confidence Factor (ECF) of 0.5 (attest-only), 0.8 (sampled), or 1.0 (verified).

ECF is applied as a multiplier to each pillar's weighted contribution, consistent with Section 6.5 of the Whitepaper:

Weighted Pillar Contribution (*Wp*) = (*Ds* ÷ 5) × *Pw* × ECF, where ***Ds*** is the pillar's average score (0–5) and ***Pw*** is the assigned weight (%).

Where ECF < 1.0, the pillar's contribution is proportionally reduced until stronger evidence is provided.

Confidence is also surfaced in reports: pillars with ECF < 1.0 may be annotated as "verification pending" until required evidence is obtained.

7. Reporting Conventions

- Pillar-level radar visualizations display the **0–5 average**.
- Overall organization score (CMI) presented as both **numeric (0–5)** and **percentage (0–100)**.
- Weighted question data, evidence links, and reviewer comments are stored for reproducibility.
- Benchmark reports compare current cycle vs previous cycle deltas per pillar.

8. Example

If *Risk & Compliance* has 12 questions totaling 48 weight points and the weighted sum of scores is 168:

Weighted Average Score = 168 ÷ 48 = 3.5

This corresponds to a **Maturity Level = 4 (Managed)**.

To normalize the result for comparison across pillars:

Normalized Pillar Score = (3.5 ÷ 5) × 100 = 70%

Therefore, the *Risk & Compliance* pillar has a **weighted maturity score of 3.5** (Level 4 – Managed) and a **normalized score of 70%** contributing to the overall Composite Maturity Index (CMI).

9. Review and Calibration

Weights and scoring algorithms are reviewed annually by the **NIRMATA Editorial Board** using aggregated pilot data to maintain fairness, prevent inflation bias, and align with evolving regulatory emphasis.

Outcome:
This standardized scoring guidance converts individual question results into a defensible, comparable, and repeatable maturity profile — the quantitative backbone of the **TRUST-IN Bharat** national benchmarking initiative.