TRUST-IN Bharat & Nirmata Framework

A whitepaper – Draft for peer review

DOCUMENT INFORMATION	
Custodian	Elytra Security
Version	v1.0 (Draft)
Revision Date	October 22, 2025
License	CC BY-SA 4.0

Contents

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

DRAFT

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Executive Overview

1. Context and Imperative

India's rapid digital expansion has transformed it into one of the world's largest generators and processors of data and users of automation, enterprise, cloud and IOT. Industrial systems, supply chains, and service platforms are now interlinked across both IT and operational technology (OT) environments. With this growth, **the scale and complexity of cyber incidents have also intensified**.

The **ENISA Threat Landscape 2025 (ETL 2025)** identifies ransomware, supply-chain compromise, and phishing as the three most significant global threat categories, noting that over **4,800 incidents** between July 2024 and June 2025 had measurable cross-sector impact. Manufacturing, public administration, and ICT services together represented more than half of reported disruptions [ENISA 2025]. Similarly, the **Verizon Data Breach Investigations Report (DBIR 2025)** finds that **human factors contributed to 70 percent of breaches**, with **phishing and credential theft** continuing to dominate initial intrusion vectors [DBIR 2025]. The **IBM X-Force Threat Intelligence Index 2025** corroborates this, ranking manufacturing as the **most attacked industry globally for the fourth consecutive year**, largely due to the operational consequences of ransomware and data-theft incidents [X-Force 2025].

Within India, the **Indian Computer Emergency Response Team (CERT-In)** has reported a sharp increase in incidents exploiting **public-facing databases, exposed ESXi servers, and insecure remote-access gateways**, as well as repeated misuse of **xp_cmdshell and PowerShell** for lateral movement [CERT-In 2024]. These findings reveal that Indian enterprises—especially those in the manufacturing and MSME sectors—face a convergence of three systemic risks:

1. **Human and cultural vulnerability**, where limited awareness undermines otherwise sound technical controls.
2. **Privacy immaturity**, with personal data protection still perceived as a compliance exercise rather than an operational discipline.
3. **Fragmented governance**, where security, risk, and privacy are managed in silos without a unifying maturity model.

The **Digital Personal Data Protection Act 2023 (DPDP Act)**, the **CERT-In Directions 2022**, and India's participation in global cybersecurity dialogues have created a foundation for national resilience. However, the absence of an integrated **maturity and trust-measurement framework** prevents consistent benchmarking across sectors, inhibiting both regulatory confidence and market assurance.

2. Purpose and Structure of the Initiative

TRUST-IN Bharat — Trusted Resilience & Unified Security Transformation for India — and the **NIRMATA Framework** together constitute a unified national initiative to **measure, improve, and demonstrate digital trust** across Indian organizations.

Component	Role	Orientation
TRUST-IN Bharat	Public-facing awareness and self-assessment programme.	Free, accessible, educational
NIRMATA Framework	Technical, evidence-based maturity and scoring model.	Standards-aligned, auditable

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

NIRMATA—**National Information Risk Maturity and Trust Assessment**—serves as the analytical engine of the initiative. It defines six maturity levels (0 to 5) and twelve assessment domains that collectively span governance, risk, compliance, privacy, AI governance, OT security, and culture. The model is designed to be:

- **Evidence-driven**, requiring verifiable documentation or control proof for every rating;
- **Cross-referenced**, aligned with **DPDP Act 2023**, **CERT-In Directions 2022**, **ISO/IEC 27001:2022**, **ISO/IEC 27701:2019**, **ISO/IEC 42001:2024**, and **NIST CSF 2.0**;
- **Sector-adaptable**, with domain weightings calibrated to sector-specific risk data;
- **Openly licensed**, published under **Creative Commons BY-SA 4.0** to encourage adoption, critique, and improvement.

3. Strategic Need for a National Baseline

India's regulatory instruments focus on *what* must be achieved—data protection, incident reporting, critical infrastructure defence—but not *how* maturity is to be measured or compared.
Without a consistent national baseline, organizations struggle to:

- Determine their relative readiness across laws and standards;
- Prioritize investments by measurable risk impact;
- Demonstrate due diligence to regulators, partners, and customers;
- Foster sector-wide improvement through benchmarking and peer learning.

Internationally, similar maturity frameworks have catalysed governance transformation: the **NIST Cybersecurity Framework**, the **FAIR model**, and **MITRE ATT&CK** have each originated as community efforts later adopted as national or international baselines. **TRUST-IN Bharat**, powered by **NIRMATA**, aspires to perform that role for India—providing a unifying, verifiable maturity scale that integrates legal, operational, and cultural dimensions of trust.

4. Manufacturing as the Pilot Sector

The initial deployment focuses on **manufacturing**, India's industrial backbone and one of the most targeted global sectors. According to **Dragos (2025)**, ransomware incidents affecting industrial organizations rose by **87 percent year-over-year**, with production interruption cited as the primary business impact. The **ENISA 2025** report similarly lists manufacturing among the top three critical-infrastructure sectors affected by cyber extortion and supply-chain compromise. In India, the **CERT-In** advisories of 2024–2025 identify manufacturing and logistics as key recipients of targeted phishing and credential attacks exploiting vendor relationships.

By applying sector-calibrated domain weights—elevating **Operational Technology & IoT Security**, **Incident Readiness**, **Culture & Awareness**, and **Privacy & Data Protection**—the framework translates international threat data into a **domestic maturity calculus**.
This ensures that assessments reflect both **global adversary trends** and **India's local regulatory environment**.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

5. Intended Outcomes

The initiative seeks to deliver five strategic outcomes:

1. **National Maturity Baseline** – a standardized scale for self-assessment and regulatory benchmarking.
2. **Cultural Transformation** – systematic integration of human-factor and privacy awareness into daily operations.
3. **Sectoral Benchmarking** – comparable maturity indices for manufacturing, IT services, and critical infrastructure.
4. **Policy Feedback Loop** – empirical evidence to inform updates to DPDP Rules, CERT-In advisories, and related standards.
5. **Global Trust Signal** – demonstrating India's commitment to responsible data and AI governance, enabling cross-border recognition and investment confidence.

6. Governance and Publication

The **Elytra Security** research group acts as framework custodian and maintains the **NIRMATA** repository and the **TRUST-IN Portal** prototype. Each release will undergo:

- **Peer review** by cross-sector experts and academic reviewers;
- **Legal and standards verification** against the latest DPDP and ISO revisions;
- **Public comment** under open license to ensure transparency and national ownership.

The whitepaper, workbook, and portal artefacts are collectively licensed under **Creative Commons BY-SA 4.0**, enabling unrestricted reuse with attribution and share-alike terms.

In essence

TRUST-IN Bharat — Trusted Resilience & Unified Security Transformation for India — powered by the NIRMATA Framework, represents India's first unified effort to convert fragmented compliance obligations into a **structured, measurable, and improvable model of digital trust**. By grounding maturity measurement in verified global intelligence and national regulatory mandates, the programme aspires to make *resilience measurable* and *trust demonstrable*—a foundational step toward a secure, privacy-respecting, and innovation-ready Digital Bharat.

7. Positioning Statement

The **TRUST-IN Bharat Framework** is **not a certification standard**, nor is it intended to replace, supersede, or conflict with any existing or emerging certification schemes such as **ISO/IEC 27001 (Information Security Management Systems)**, **ISO/IEC 27701 (Privacy Information Management)**, **ISO/IEC 42001 (Artificial Intelligence Management Systems)**, **SOC 2**, or any framework recognized by the **Bureau of Indian Standards (BIS)** or other international accreditation bodies.

Instead, TRUST-IN Bharat functions as an **independent maturity and readiness assessment framework -** a structured, evidence-based tool that helps organizations understand **where they currently stand** in relation to globally accepted standards and **what actions** are necessary to achieve formal certification, should they choose to pursue it.

It enables **progressive, proportional adoption**, particularly for **MSMEs and mid-sized enterprises**, guiding them through a clear, measurable path from **awareness** to

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

sustained compliance without the administrative or financial burden typically associated with certification programs.

At its present stage, TRUST-IN Bharat serves as an **advisory and capability-building initiative** designed to **complement** and **support** recognized standards by offering **clarity, structure, and measurable maturity guidance** to Indian organizations. If, in the future, the **Bureau of Indian Standards (BIS)** or another competent authority reviews and formalizes its methodology, it may evolve into a **nationally recognized certification program** in its own right. Until such formal adoption, its role remains **informative, non-accredited, and supportive**.

8. Legal & Attribution Note

The **TRUST-IN Bharat Framework** and the **NIRMATA Maturity Model** are original works authored and published under the **Creative Commons Attribution–ShareAlike 4.0 International License (CC BY-SA 4.0)**. They are provided **for guidance and educational purposes only** and **do not confer or imply certification, accreditation, or endorsement** by any standards body or regulatory authority. Organizations remain solely responsible for ensuring conformance with applicable legal, regulatory, and certification requirements.

Introduction and Rationale

1. The Evolving Landscape of Digital Risk in India

India's economic transformation is inseparable from its rapid digitalization. As of 2025, the country hosts one of the world's largest data ecosystems—spanning financial technology, e-governance, manufacturing automation, logistics, and artificial intelligence (AI) deployment. Industrial and service organizations alike depend on connected IT–OT networks, multi-cloud architectures, and data-driven decision systems. This integration has increased efficiency and innovation but has also **multiplied systemic exposure** to cyber and privacy risks.

1.1 Global threat intelligence convergence

According to the **ENISA Threat Landscape 2025**, ransomware continues to dominate global impact statistics, accounting for approximately **46 percent of reported cyber incidents** during July 2024–June 2025. ENISA further notes a marked rise in **multi-stage supply-chain compromise** and the increasing exploitation of **legitimate remote-management tools**—an evolution that blurs the boundary between cybercrime and state-linked intrusion campaigns [ENISA 2025].

The **Verizon DBIR 2025** corroborates this trajectory:

- **Human factors** remain present in **seven of ten breaches**,
- **Phishing** is still the primary initial access vector, and
- **Credential theft** drives the majority of lateral-movement activity [DBIR 2025].

The **IBM X-Force Threat Intelligence Index 2025** confirms that **manufacturing remains the most attacked industry for the fourth consecutive year**, with **26 percent of all ransomware incidents** targeting industrial organizations [X-Force 2025]. Dragos' *Industrial Ransomware Report 2025* quantifies this surge at **1,693 industrial ransomware cases worldwide**—an **87 percent year-over-year increase**, where production stoppage and reputational damage outweighed data loss as the principal business impacts [Dragos 2025].

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

1.2 National threat posture

India mirrors these global patterns. **CERT-In's 2024–2025 advisories** highlight consistent exploitation of:

- Public-facing SQL and NAS servers via weak credentials,
- Unpatched virtualization platforms (notably ESXi and Hyper-V), and
- Misconfigured cloud storage buckets.

These incidents frequently use **PowerShell**, **WMIC**, and **xp_cmdshell** for lateral propagation—tactics identical to those observed in global ransomware campaigns [CERT-In 2024].

The **Picus Blue Report 2025** reinforces another dimension: the **ineffectiveness of many deployed security controls**. Across a corpus of 15 million simulated attacks, only **43 percent** were detected or prevented at the first layer of defense [Picus 2025]. This empirical finding underscores a chronic gap between policy intent and technical execution—amplified in sectors where operational technology and legacy systems coexist.

2. Drivers for a Unified Maturity Baseline

2.1 Fragmented frameworks and compliance fatigue

Indian organizations presently navigate a patchwork of overlapping mandates:

- The **Digital Personal Data Protection Act 2023** demands lawful processing, consent governance, and grievance redressal.
- The **CERT-In Directions 2022** impose six-hour incident-reporting timelines, log-retention, and synchronization obligations.
- Sectoral regulators such as **RBI**, **IRDAI**, and **SEBI** have parallel information-security guidelines.

While these instruments define compliance requirements, none prescribes a common method for **measuring maturity** or **benchmarking resilience**. Consequently, organizations expend effort on audit checklists rather than continuous improvement.

This gap widens when small and medium enterprises—particularly in manufacturing—lack in-house expertise to interpret standards such as **ISO/IEC 27001:2022**, **ISO/IEC 27701:2019**, or **NIST CSF 2.0**.

2.2 The need for measurable trust

Globally, policymakers are converging on **outcome-based assurance**. ENISA 2025 emphasises "measurable resilience indicators" for member states; the **NIST CSF 2.0** introduces "Govern" as a core function to connect executive oversight with measurable control performance [NIST 2024]. Within India, the DPDP Act's obligations—such as purpose limitation, consent traceability, and grievance closure—necessitate quantifiable metrics to evidence accountability. Without such a scale, compliance remains subjective, undermining trust between regulators, enterprises, and citizens.

2.3 Human and privacy deficits as structural risks

The **DBIR 2025** attributes nearly **one-third of confirmed breaches** to social engineering alone. In India, workforce diversity, contract-based employment, and low baseline cyber hygiene exacerbate this exposure. Meanwhile, **privacy literacy** within enterprises remains nascent. The DPDP Act's introduction marks the first legal recognition

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

of data-subject rights in India, yet most manufacturing and MSME organizations have no operational process for consent capture, notice, or data-subject-request management. This creates a two-fold deficit—*human* and *privacy*—that traditional information-security audits fail to measure.

3. Rationale for NIRMATA and TRUST-IN Bharat

TRUST-IN Bharat — Trusted Resilience & Unified Security Transformation for India—addresses this national need for an integrated maturity and awareness programme. Its underlying **NIRMATA Framework (National Information Risk Maturity and Trust Assessment)** operationalizes three strategic design aims:

1. **Unification:** Establish a single maturity lexicon spanning governance, risk, privacy, and AI governance, reducing audit duplication.
2. **Verification:** Anchor self-assessment in verifiable evidence, not perception, through structured scoring and confidence factors.
3. **Adaptation:** Tailor domain weightings to sectoral risk signals—beginning with manufacturing—using live intelligence from ENISA 2025, X-Force 2025, Dragos 2025, and CERT-In 2024–25.

The framework transforms abstract regulatory compliance into **a measurable model of trustworthiness**, supporting both voluntary disclosure and potential alignment with BIS LITD 27 standards activity.

4. Expected Policy and Industry Benefits

Stakeholder	Benefit
Enterprises and MSMEs	Consistent self-assessment scale; evidence templates; roadmap for resilience improvement.
Regulators and Policymakers	Empirical maturity data to calibrate policy interventions and update guidance.
Industry Associations	Benchmark datasets for awareness campaigns and sector-wide reporting (“State of Trust in Bharat” index).
Certification Bodies and Auditors	Common maturity vocabulary aligning with ISO 27001, 27701, 42001, and NIST CSF 2.0, enabling audit interoperability.
Academia and Research	Open data corpus for longitudinal studies on cyber-risk evolution and privacy adoption.

5. Positioning within the Global Trust Ecosystem

By unifying governance, privacy, and AI risk under a single maturity model, **TRUST-IN Bharat** positions India alongside jurisdictions that have institutionalized trust measurement.
Comparable initiatives include:

- The **EU Cybersecurity Maturity Framework (ENISA 2025 reference)**,
- The **U.S. Cybersecurity Framework 2.0 (NIST 2024)**, and
- The **Singapore Cybersecurity Labelling Scheme** for IoT safety.

Yet, **NIRMATA** differs in two critical ways:

1. It integrates **privacy and human-factor dimensions** as core maturity determinants, not peripheral annexes.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India’s DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

2. It is **openly licensed (CC BY-SA 4.0)** to foster public–private collaboration and voluntary adoption before formal standardization.

6. Conclusion

India stands at an inflection point: legislative progress in data protection has outpaced the operational ability of enterprises to demonstrate compliance through measurable trust indicators.
Without a unified maturity baseline, national cyber-resilience efforts remain fragmented and reactive. By grounding its assessment logic in validated global threat intelligence and domestic regulatory mandates, **TRUST-IN Bharat**, powered by **NIRMATA**, offers a structured pathway from awareness to assurance—enabling organizations to transform *compliance* into *confidence* and to make *trust* a measurable asset of India's digital economy.

Design Principles

1. Foundational Philosophy

The **NIRMATA Framework** and the **TRUST-IN Bharat — Trusted Resilience & Unified Security Transformation for India** programme are founded on the principle that *trust* is not an abstract value but a measurable outcome of design, governance, and behavior.
The framework translates this philosophy into three mutually reinforcing design tenets: **Trust by Design**, **Privacy by Design**, and **Resilience by Default**. These principles align with international standards—**ISO/IEC 27001:2022**, **ISO/IEC 27701:2019**, **ISO/IEC 42001:2024**, and **NIST CSF 2.0**—and with the national imperatives defined by the **Digital Personal Data Protection Act 2023** and the **CERT-In Directions 2022**.

Each tenet is both **aspirational** (defining the maturity ideal) and **operational** (providing measurable control objectives). Together, they form the normative backbone of NIRMATA's domain taxonomy and scoring model.

2. Trust by Design

2.1 Definition

Trust by Design is the architectural integration of transparency, accountability, and verifiability into all systems, processes, and decision pathways that handle information. It recognizes that trust is built through *observable assurance*—the ability of stakeholders to verify that governance, risk, and security claims are substantiated by evidence.

2.2 Rationale

The **ENISA Threat Landscape 2025** highlights "trust erosion through opacity" as a recurring challenge: organizations frequently deploy security technologies without disclosing governance or validation mechanisms, leading to confidence deficits in supply-chain relationships [ENISA 2025]. Similarly, the **Picus Blue Report 2025** finds that **57 percent of enterprises overestimate the effectiveness of their controls**, revealing a perception–reality gap that undermines assurance [Picus 2025].

Trust by Design therefore mandates that systems and processes be **auditable, explainable, and evidence-backed** at every stage.

2.3 Core Attributes

Attribute	Description	Example Metrics / Evidence
Transparency	Documented policies, roles, and data flows visible to	Published governance charters; accountability matrices.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

	stakeholders.	
Accountability	Named owners for each control and risk area.	Responsibility traceability logs; approval trails.
Verifiability	Independent mechanisms to test control effectiveness.	Audit trails, penetration-test reports, control-effectiveness testing (Picus simulations).
Consistency	Alignment between declared policy and observed behavior.	Periodic reconciliation between risk register and implemented controls.

2.4 Alignment References

- **NIST CSF 2.0 — Govern Function**: defines governance integration and communication of cybersecurity risk.
- **ISO/IEC 27001:2022 Clauses 5–10**: mandates accountability, documentation, and continual improvement.
- **ENISA 2025 Theme "Visibility and Assurance"**: underlines transparency as a determinant of stakeholder confidence.

3. Privacy by Design

3.1 Definition

Privacy by Design embeds personal-data protection and ethical handling into every stage of system and process development—from data collection to deletion—ensuring that privacy becomes a structural property, not an afterthought.

3.2 Rationale

The **Digital Personal Data Protection Act 2023** codifies privacy as a statutory duty and introduces explicit obligations for consent, purpose limitation, and grievance redressal. Yet, the **DBIR 2025** and **X-Force 2025** both indicate that misconfigurations, excessive data retention, and insider misuse remain prevalent. The **ENISA 2025** report expands this view, noting a sharp rise in **"data leakage without intrusion"** incidents—cases where privacy harm occurred without system compromise [ENISA 2025].

Privacy by Design responds by integrating **lawfulness, necessity, and proportionality** into the design and operation of data systems.

3.3 Core Attributes

Attribute	Description	Implementation Evidence
Lawfulness and Fairness	Data processed with clear legal basis and consent.	Consent records; lawful basis registry; DPIA reports.
Purpose Limitation and Minimization	Data collected only for defined purposes, stored minimally.	Data inventory and retention matrix; deletion logs.
Transparency and Rights Enablement	Clear notices, accessible grievance and DSR mechanisms.	Privacy notices; DSR closure logs; DPO dashboards.
Security and Accountability	Integration with ISMS and privacy KPIs.	Mapped control catalogue; privacy audit findings.

3.4 Alignment References

- **DPDP Act 2023** – Sections 4–9 (duties of data fiduciaries, consent, DSR).

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- **ISO/IEC 27701:2019 Clauses 5–7** – Privacy Information Management System.
- **ISO/IEC 42001:2024 Clauses 4.2 & 6.2** – Ethical AI and personal-data considerations in model lifecycle.
- **ENISA 2025 "Data Exposure and AI Privacy" section** – highlights the link between data governance and model safety.

4. Resilience by Default

4.1 Definition

Resilience by Default means that systems and processes are architected to **anticipate, withstand, recover from, and adapt to** adverse events—be they cyber incidents, privacy violations, or AI failures—without reliance on ad-hoc human intervention.

4.2 Rationale

Resilience has become the defining metric of maturity. The **Dragos Industrial Ransomware Report 2025** confirms that organizations with tested recovery plans restored operations **52 percent faster** than those relying on reactive containment. The **ENISA 2025** report similarly observes that entities with automated incident detection and continuity planning had **40 percent lower mean downtime** after ransomware events.
These findings validate the need for resilience to be *designed-in* rather than retrofitted.

4.3 Core Attributes

Attribute	Description	Indicators
Anticipation	Proactive identification of risks and dependencies.	Threat modelling; red-teaming; tabletop exercises.
Withstanding	Containment capability without cascading impact.	Segmentation metrics; OT network isolation scores.
Recovery	Documented and tested continuity plans.	Recovery Time Objective (RTO); drill records.
Adaptation	Continuous learning and improvement loop.	Post-incident review reports; updated playbooks.

4.4 Alignment References

- **CERT-In Directions 2022** – incident reporting, logging, and retention obligations.
- **ISO/IEC 27001:2022 Annex A.17** – information security continuity.
- **NIST CSF 2.0 "Recover" Function** – establishes organizational recovery outcomes.
- **ENISA 2025** – cross-sector findings on downtime reduction via preparedness.

5. Interdependency of the Three Tenets

The three tenets are **mutually reinforcing** rather than sequential:

Tenet	Primary Objective	Enables
Trust by Design	Transparency and accountability	Verification and assurance
Privacy by Design	Lawfulness and fairness	Ethical data governance
Resilience by Default	Continuity and adaptation	Sustainable confidence

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Their intersection defines **organizational digital trust maturity**. Trust cannot be sustained without privacy; privacy cannot be ensured without resilience; resilience cannot be demonstrated without trustworthiness. The **NIRMATA Framework** integrates these tenets through its domain taxonomy—embedding their measurable indicators within the **12 NIRMATA domains** and corresponding **0–5 maturity ladder**.

6. Conclusion

The design principles of **Trust by Design**, **Privacy by Design**, and **Resilience by Default** constitute the normative and ethical foundation of the NIRMATA Framework. They translate India's legislative and operational aspirations into actionable engineering and governance practices—ensuring that **TRUST-IN Bharat** assessments do not merely score compliance but also evaluate an organization's ability to sustain verifiable trust under continuous change. These tenets establish the bridge between law, technology, and behavior—the three pillars upon which a **Secure and Trusted Digital Bharat** must stand.

The Twelve NIRMATA Domains (Pillars of Trust)

1. Governance & Leadership

Definition

Governance & Leadership define how an organization's leadership establishes, directs, and sustains its information-risk, privacy, and AI-governance objectives. It encompasses board-level ownership, funding, policies, charters, and documented responsibilities that connect business strategy to trust outcomes.

Rationale

The **Verizon DBIR 2025** and **IBM X-Force 2025** both conclude that lack of executive sponsorship remains a leading root cause of repeated incidents—organizations without defined governance functions were **2.5 times more likely** to experience recurring compromise.
In India, the **DPDP Act 2023** and **CERT-In Directions 2022** assign explicit accountability to "data fiduciaries" and "reporting entities," making governance a statutory obligation rather than a best practice.

Alignment

- **ISO/IEC 27001 Clauses 5–10** – Leadership, Planning, Operation, Performance Evaluation, Improvement.
- **NIST CSF 2.0 – Govern Function** – establishing and communicating cybersecurity risk management.
- **DPDP Act 2023 Sections 9–10** – Duties of data fiduciaries and appointment of Data Protection Officer.

Indicative Evidence

- Board-approved information-security and privacy policies.
- Defined CISO/DPO/AI-Governance roles with budgets and KPIs.
- Governance committee minutes and risk-reporting dashboards.
- Annual management review outcomes and improvement actions.

Interlinkages

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Governance & Leadership underpin all other pillars by enabling prioritization and resourcing; it directly influences **Risk Management**, **Compliance Management**, and **Culture & Awareness**.

2. Risk & Compliance

Risk Management

Definition

Risk Management is the systematic process of identifying, assessing, prioritizing, and mitigating risks that affect confidentiality, integrity, availability, and lawful use of information and AI assets across IT, OT, and cloud environments.

Rationale

The **ENISA Threat Landscape 2025** emphasizes that **risk quantification and contextual awareness** are key differentiators of mature organizations: enterprises with continuous risk registers experienced **40 % fewer unplanned outages** than those relying on ad-hoc assessments [ENISA 2025]. In the Indian context, risk management is integral to **CERT-In Direction (2)**—requiring entities to maintain logs and incident analysis capabilities—and to ISO's continuous-improvement cycle.

Alignment

- **ISO/IEC 27005:2022** – Information-security risk management methodology.
- **NIST CSF 2.0 – Identify Function** – Asset, Business, and Risk Assessment categories.
- **CERT-In Directions 2022 Clauses (i) & (ii)** – log retention and vulnerability assessment.

Indicative Evidence

- Enterprise and plant-level risk registers linked to controls.
- Periodic risk assessments with quantification or heat-map outputs.
- Documented treatment plans and residual-risk acceptance records.
- Integration of privacy and AI-ethics risks into enterprise GRC systems.

Interlinkages

Feeds directly into **Governance & Leadership** for oversight, informs **Incident Readiness**, and supports **Metrics & Monitoring** by providing baseline measures for improvement tracking.

Compliance Management

Definition

Compliance Management ensures adherence to applicable legal, regulatory, contractual, and internal policy requirements relating to data protection, cybersecurity, and AI governance. It converts statutory obligations into actionable control objectives with mapped evidence.

Rationale

Organizations face overlapping mandates—**DPDP Act 2023**, **CERT-In Directions 2022**, sectoral RBI/IRDAI/SEBI norms, and international export-control or privacy rules. Without centralized compliance mapping, duplicated audits cause fatigue and inefficiency.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

ENISA 2025 cites fragmented compliance as a leading cause of "audit blindness," where organizations remain non-compliant despite certification [ENISA 2025].

Alignment

- **ISO/IEC 37301:2021** – Compliance Management Systems.
- **DPDP Act 2023 Sections 8–10** – Duties of data fiduciaries, consent and grievance.
- **CERT-In Directions 2022** – Mandatory incident reporting within six hours.
- **NIST CSF 2.0 – Govern & Identify** functions (Regulatory Requirements category).

Indicative Evidence

- Compliance register covering DPDP, CERT-In, ISO controls, and contracts.
- Audit calendar and internal-control testing results.
- Evidence retention and legal-hold policy.
- Regulator or client compliance-attestation reports.

Interlinkages

Compliance Management operationalizes **Governance** directives and validates outcomes from **Risk Management**; it shares artefacts with **Privacy & Data Protection** and **Vendor Governance** for processor accountability.

3. Application and Product Security

AI Governance & Ethical Use

Definition

AI Governance & Ethical Use ensures that artificial-intelligence and machine-learning systems are developed and operated with fairness, transparency, accountability, and security.
It addresses risks arising from bias, model drift, data leakage, adversarial manipulation, and regulatory non-compliance.

Rationale

AI is rapidly permeating industrial operations—from predictive maintenance and quality control to HR analytics.
The **ENISA Threat Landscape 2025** identifies AI supply-chain compromise and data-poisoning as emerging risks, while the **ISO/IEC 42001:2024** introduces the world's first formal standard for AI management systems. India's DPDP Act implicitly extends privacy obligations to AI data processing, reinforcing the need for AI-specific governance.

Alignment

- **ISO/IEC 42001:2024** – Artificial Intelligence Management System.
- **ENISA 2025 AI & Emerging Technologies Section** – Model manipulation and bias findings.
- **DPDP Act 2023 Sections 4–9** – Lawful basis, fairness, and transparency obligations.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- **NIST AI Risk Management Framework (RMF 1.0)** – trustworthy AI principles (referential).

Indicative Evidence

- AI system inventory with risk classification and ownership.
- Documented model-training data provenance and bias testing results.
- AI incident register and review committee minutes.
- Explainability documentation for high-impact models.

Interlinkages

Integrates with **Data Lifecycle & Classification** (for training-data hygiene), **Privacy & Data Protection** (for lawful processing), and **Metrics & Continuous Improvement** (for model drift and bias monitoring). It completes the NIRMATA model's coverage of the **trust–privacy–resilience** continuum by extending maturity measurement into the AI era.

4. Asset & Data Management

Definition

Data Lifecycle & Classification governs how data is created, labeled, stored, used, shared, retained, and disposed of to ensure lawfulness, proportionality, and security. It anchors *Privacy by Design* by embedding control at the data element level.

Rationale

1. The **DBIR 2025** notes that **data mis-handling and excessive retention** contribute to 22 % of confirmed breaches.
2. The **ENISA 2025** report similarly highlights **"data sprawl"** as a major enabler of AI-driven data leakage incidents.
3. Under the **DPDP Act 2023**, improper classification or retention beyond lawful purpose constitutes a compliance violation.

Hence, classification and lifecycle control are preconditions for both cybersecurity and privacy assurance.

Alignment

- **ISO/IEC 27701:2019 § 6.8** – Information classification and retention.
- **DPDP Act 2023 Sections 5–9** – Purpose limitation, storage limitation, and accuracy.
- **NIST CSF 2.0 – Protect Function** – Data security category.

Indicative Evidence

- Data inventory and classification schema approved by leadership.
- Retention and deletion schedules linked to system enforcement logs.
- Encryption and DLP configuration baselines mapped to classification levels.
- Records of anonymization or pseudonymization for high-risk datasets.

Interlinkages

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Provides foundational input to **Privacy & Data Protection** (consent and DSR handling) and to **AI Governance** (training-data provenance). Strong classification supports **Incident Readiness** by enabling targeted containment of sensitive datasets.

5. Identity & Access

Definition

Identity & Access (AIM) governs authentication, authorization, and privilege enforcement across IT, OT, and cloud environments. Its purpose is to ensure that only verified and authorized individuals or systems access organizational resources, thereby minimizing identity-centric compromise.

Rationale

1. The **Verizon DBIR 2025** attributes **61 percent of breaches** to credential theft, privilege misuse, or misconfigured access paths.
2. **ENISA 2025** identifies credential compromise as the **top vector** for initial intrusion across all sectors, including manufacturing.
3. In India, CERT-In advisories repeatedly highlight weak administrative credentials, shared accounts, and inadequate MFA as leading causes of exploitation. Hence, AIM maturity is the cornerstone of both cybersecurity and privacy assurance.

Alignment

- **ISO/IEC 27001:2022 Annex A.5–A.9** – Access control and identity management.
- **NIST CSF 2.0 – Protect Function** – Identity management, authentication, and access control.
- **CERT-In Direction (2)** – Accountable logging and traceability of user activities.
- **DPDP Act 2023 Section 9** – Security safeguards for personal data.

Indicative Evidence

- MFA and just-in-time privilege provisioning logs.
- Role-based access control (RBAC) matrix with periodic reviews.
- PAM system reports; joiner–mover–leaver records.
- Segregation-of-duties analysis for high-risk functions.

Interlinkages

Identity & Access is a direct enabler for **Governance**, **Operational Technology & IoT Security**, and **Privacy & Data Protection**. It also supplies key telemetry to **Metrics & Continuous Improvement** for access-anomaly monitoring.

6. Infrastructure Security

Infrastructure Security covers enterprise IT and plant-level OT/IIoT. All OT/IIoT requirements are assessed under the subsection ‘Operational Technology & IoT Security’ in this pillar. Controls reference sector guidance (e.g., IEC 62443 families) by citation only; we avoid reproducing proprietary text.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India’s DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Operational Technology & IoT Security

Definition

Operational Technology (OT) & IoT Security focuses on safeguarding industrial systems, connected sensors, and control environments from cyber-physical threats. It ensures that safety, reliability, and production continuity are not compromised by digital attacks.

Rationale

The **IBM X-Force Threat Intelligence Index 2025** designates **manufacturing as the most attacked industry** globally, while **Dragos 2025** reports a year-on-year **87 percent surge in industrial ransomware incidents**. In many Indian manufacturing plants, legacy OT systems remain unpatched or are remotely accessible through insecure channels. These environments require specialized segregation, firmware integrity validation, and secure OEM access management. The **ENISA 2025** and **CERT-In 2024–25** bulletins confirm that convergence of IT and OT networks without corresponding controls amplifies systemic risk.

Alignment

- **IEC 62443 Series** – Industrial automation and control system security.
- **NIST CSF 2.0 – Identify, Protect, and Respond Functions.**
- **CERT-In Directions 2022** – Incident logging and reporting for critical systems.
- **ISO/IEC 27019:2022** – Security management for energy and industrial control systems.

Indicative Evidence

- Updated OT/IoT asset inventory and network segmentation diagrams.
- OEM remote-access authorization and monitoring records.
- Patch and firmware validation reports; configuration baselines.
- Incident drills simulating OT disruption or ransomware scenarios.

Interlinkages

Integrates tightly with **Incident Readiness** for recovery, with **Identity & Access** for privileged control, and with **Risk Management** for systemic threat modeling.

7. Supply-Chain Security

Definition

Supply-Chain Security covers the full lifecycle of third-party and fourth-party relationships that can affect our confidentiality, integrity, availability, and compliance posture. It includes due diligence, contractual controls, secure onboarding and access, continuous assurance, software supply-chain integrity (SBOM/provenance), coordinated incident handling, and secure termination with data return or deletion.

1. Supplier Inventory & Tiering

Define how vendors/partners are discovered, recorded, and risk-tiered (critical/high/medium/low) based on data sensitivity, access, and service criticality.

2. Due Diligence & Approval

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Security, privacy, and financial screening before engagement. Use standardized questionnaires where applicable and require evidence for critical vendors.

3. Contractual & Legal Controls

Data Processing Agreements, SLAs/SLOs, breach-notification timelines, right-to-audit, sub-processor disclosure, flow-down clauses, data location, and exit/transition terms.

4. Onboarding & Access Provisioning

Least-privilege access, time-bound or purpose-bound credentials, JML for vendor personnel, network segmentation, and monitoring hooks established at onboarding.

5. Continuous Monitoring & Assurance

Evidence refresh cadence by tier (e.g., annual for high/critical): certificates/attestations, pen-test summaries, patch/vulnerability advisories, and material change notifications.

6. Software Supply Chain Integrity

SBOM collection, update cadence, provenance/attestations (e.g., signed builds, artifact verification), vulnerability disclosures (VEX) and remediation expectations for embedded/open-source components.

7. Fourth-Party/Sub-processor Oversight

Visibility into sub-processors for critical vendors and enforcement of flow-down requirements proportionate to risk.

8. Joint Incident Handling & Notifications

Bidirectional notification windows, joint playbooks/RACI, escalation paths, and evidence exchange during incidents affecting our data or services.

9. Termination, Offboarding & Data Disposition

Credential revocation, asset return, certified deletion/return of data, and transition support for critical services.

Rationale

The **ENISA Threat Landscape 2025** ranks **supply-chain compromise** as the second most impactful threat class globally, following ransomware. Breaches such as MOVEit (2023) demonstrated that single-point third-party failures can cascade across thousands of organizations. The **DPDP Act 2023** makes data fiduciaries responsible for their processors' actions, creating legal accountability for vendor lapses. Therefore, a structured supply-chain-governance program is essential for risk containment.

Alignment

- **ISO/IEC 27036:2021** – Information-security supplier-relationship management.
- **DPDP Act 2023 Section 8(6)** – Accountability of data fiduciary for processor compliance.
- **NIST CSF 2.0 – GV.SC (Supply-Chain Risk Management)**
- **ISO/IEC 27001:2022 - A.5.20 Supplier relationships; A.5.21 Managing information security in the ICT supply chain**
- **ENISA 2025** – Cross-sector findings on supplier compromise trends.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Indicative Evidence

- Vendor risk-assessment questionnaires and scoring.
- Security and privacy clauses in contracts and NDAs.
- Annual reassessment or attestation reports.
- Joint incident-response playbooks with strategic suppliers.

Interlinkages

Relies on **Governance & Leadership** for policy and ownership, and on **Risk & Compliance** for legal/regulatory oversight; feeds **Incident Readiness** for coordinated containment and **Business Continuity & Resilience** for alternate supplier/exit planning.

Evidence & assurance artifacts

Maintain and, for high/critical vendors, periodically refresh:

- Executed DPA and information security addendum
- Current SOC 2 / ISO 27001/27701 certificate or equivalent attestation (validity dates)
- Third-party pen-test or independent assessment summaries (redacted)
- SBOM and, where available, VEX statements; build/provenance attestations for delivered software
- Security questionnaire responses and remediation plans
- Right-to-audit confirmations or audit reports (as applicable)
- Incident notification records and post-incident reports (if any)
- Offboarding confirmations for data return/deletion

8. Incident Readiness

Definition

Incident Readiness (IR) establishes the structured capability to detect, assess, contain, and recover from security or privacy incidents while maintaining essential operations. It emphasizes preparation (roles, playbooks, exercises), rapid decision-making, and continuous learning from events. (Continuity/DR specifics are addressed under Business Continuity & Resilience.)

Rationale

The **ENISA Threat Landscape 2025** reports that **mean downtime from ransomware incidents** decreased by **40 percent** among organizations with tested response plans. **Dragos 2025** similarly finds that plants with integrated IT-OT continuity planning resumed operations **52 percent faster** than reactive peers. In India, **CERT-In Directions 2022** require incident reporting within six hours - non-compliance can attract enforcement. Organizations with tested response plans consistently resume operations faster and limit business impact. A well-governed IR function is therefore essential to legal compliance and operational stability.

Alignment

- **ISO/IEC 27035:2023** – Information-security incident-management principles.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- **CERT-In Directions 2022 (Clauses iii–iv)** – Incident classification and reporting timelines.
- **NIST CSF 2.0 – Respond and Recover Functions.**
- (See Business Continuity & Resilience for ISO/IEC 22301 alignment)

Core Capabilities

- Detection & Triage — Clear intake channels, severity classification, and escalation paths
- Roles, RACI & Playbooks — Named responders, decision authorities, and scenario-specific procedures (e.g., ransomware, data leakage, supplier breach)
- Containment & Eradication — Short-term containment, root-cause remediation, hardening to prevent re-occurrence
- Forensics & Evidence Handling — Evidence preservation, chain-of-custody, and tooling to support investigations and legal process
- Communications & Notifications — Internal comms, executive briefings, regulator/customer/vendor notifications (including CERT-In timelines where applicable)
- Post-Incident Review & Improvement — Lessons learned, corrective/preventive actions (CAPA), and updates to controls, playbooks, and training

Indicative Evidence

- Approved, version-controlled Incident Readiness policy and playbooks
- Incident register with root-cause analyses, CAPA, and closure status
- Exercise records (e.g., quarterly tabletop, red/blue/purple-team), including after-action reports
- Contact lists and on-call schedules; delegation of authority
- Notification logs (e.g., CERT-In/sectoral/regulatory, customer/vendor) and time-stamped submissions
- Tooling evidence: alert tickets, case files, forensic collections, and linkage to detections (SIEM/SOAR)

Interlinkages

This pillar relies on **Monitoring & Detection** for timely alerting and signal quality; coordinates with **Governance & Leadership** for authority and oversight; with **Risk & Compliance** for statutory/contractual obligations; with **Supply-Chain Security** for vendor-led incidents; and with **Business Continuity & Resilience** for recovery strategies and continuity objectives.

9. Business Continuity & Resilience

Definition

Business Continuity & Resilience (BR) ensures the organization can maintain or rapidly restore prioritized services when disruptive events occur. It translates business impact into

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

recovery objectives, defines continuity strategies and workarounds, and proves recoverability through planned exercises and real-world learning.

Rationale

Continuity planning protects customers, revenue, and safety when technology, facilities, people, or key suppliers fail. By setting clear recovery objectives (RTO/RPO), validating backups and failover paths, and practicing realistic scenarios, the organization reduces downtime and avoids improvisation during crises.

Alignment

• ISO 22301:2019 — Business continuity management systems

• ISO/IEC 27031 — ICT readiness for business continuity

• NIST SP 800-34 — Contingency Planning Guide for Information Systems

• NIST CSF 2.0 — Recover (RC) Function

Core Capabilities

• Business Impact Analysis (BIA) & Dependencies — Identify critical processes, upstream/downstream dependencies, and minimum service levels.

• Recovery Objectives — Set and maintain RTO/RPO and Maximum Tolerable Downtime (MTD) per process/system.

• Continuity Strategies & Workarounds — Define alternate sites, manual procedures, and substitution options for people, tech, and suppliers.

• DR Architecture & Resilience Patterns — Design for recoverability (e.g., active/active, warm standby, segmented restores) with documented runbooks.

• Backups & Restoration — Retention/immutability, offline/off-cloud copies, periodic restore tests (sampled and full), integrity verification.

• Plans, Roles & Communications — Approved continuity/DR plans, crisis roles and call trees, stakeholder messaging templates.

• Exercises & Validation — Tabletop drills, technical failovers, unannounced restore tests; track issues to closure.

• Supplier Continuity & Exit — Validate critical vendors' continuity posture; maintain tested exit plans and alternates (ties to Supply-Chain Security).

• Post-Event Review & Improvement — Capture lessons learned, update BIAs, plans, runbooks, and training.

Indicative Evidence

• Approved BIA register with current criticality tiers and RTO/RPO/MTD.

• Continuity/DR plans and system-level recovery runbooks.

• Backup reports (success rates, retention, immutability) and restoration test records.

• Exercise/Failover reports with corrective actions and retest results.

• Crisis contact lists, call-tree tests, and communication templates.

• Supplier continuity attestations/assessments for critical services; exit/transition plans.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Interlinkages

Coordinates with Incident Readiness for handoffs from containment to recovery; with Infrastructure Security for recovery architecture and backups; with Supply-Chain Security for alternates and concentration risk; and with Governance & Leadership for authority, priorities, and funding.

10. Privacy & Data Protection

Definition

Privacy & Data Protection translates the **Digital Personal Data Protection Act 2023 (DPDP Act)** 2023's principles into daily, measurable practice—including consent management, Data Principal Rights, grievance redressal, cross-border transfers (as permitted), and privacy-by-design. This domain encompasses consent management, data-principal-rights (DPR) handling, grievance redressal, lawful cross-border transfers, and privacy-by-design enforcement within business processes.

Rationale

Privacy has become the cornerstone of public trust.
The **ENISA Threat Landscape 2025** highlights "data exposure without intrusion" and "AI-driven data leakage" among the most impactful risks, showing confidentiality failures often stem from process gaps rather than intrusions.
In India, where the DPDP Act has introduced explicit rights for individuals and duties for organizations, operationalizing privacy is no longer discretionary.
However, awareness remains low: most manufacturing and MSME organizations have not yet implemented structured DSR workflows or consent registries, leaving them non-compliant by default.

Alignment

- **DPDP Act 2023 Sections 4–10** – Duties of data fiduciaries, rights of data principals, and consent.
- **ISO/IEC 27701:2019 Clauses 5–7** – Privacy Information Management Systems.
- **NIST CSF 2.0 "Govern" Function** – Govern (GV) function (privacy-related outcomes)
- **ENISA 2025** – Trends in personal-data exposure and AI privacy challenges.

Indicative Evidence

- Consent-capture logs linked to purpose identifiers.
- DSR and grievance closure reports within statutory timelines.
- Records of privacy-impact assessments (PIAs/DPIAs).
- Cross-border transfer approvals and contractual safeguards repository (as applicable under DPDP and other regimes).

Interlinkages

Works with **Governance & Leadership** (accountability), **Risk & Compliance** (legal basis, notifications), **Asset & Data Management** (classification, retention), **Identity & Access** (least privilege, auth), **Supply-Chain Security** (processor controls), **Monitoring & Detection** (logs/alerts), and **Incident Readiness** (privacy incident response).

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

11. Culture, Training & Awareness

Definition

Culture, Training & Awareness measures how effectively an organization embeds security, privacy, and ethical-behavior principles into its workforce and contractor ecosystem. It represents the "human firewall" dimension of trust maturity. Scope includes role-based training (including secure engineering and privacy), simulations (e.g., phishing, tabletop), onboarding/offboarding requirements, contractor coverage, and measurement of training effectiveness.

Rationale

The **Verizon DBIR 2025** attributes **70 percent of breaches** to human factors, while **ENISA 2025** cites social engineering and phishing as the **most common initial intrusion methods**. In manufacturing, heterogeneous workforces—often comprising contractors and shop-floor technicians—face unique awareness challenges. Behavioural maturity is thus as critical as technical control maturity. Embedding awareness directly supports the DPDP Act's emphasis on grievance prevention and responsible data handling.

Role-based Training & Frequency

Baseline plus role-specific paths (engineering/secure coding, OT/plant operations, privacy/DPO/helpdesk), refresher cadence, and contractor/vendor inclusion.

Simulations & Exercises

Phishing/social-engineering campaigns and IR tabletops tied to top risks; document outcomes and remediation follow-ups.

Reporting Culture ("Speak-up", No-blame)

Anonymous channels, non-retaliation, near-miss reporting, and leadership tone; encourage early escalation over silent failure.

Effectiveness & Metrics

Training completion and assessment rates; phishing report vs. click-through rates; time to remediate findings; trend reviews feeding program updates.

Alignment

- **ISO/IEC 27001:2022 Annex A.6 & A.7** – Human resource security and awareness training.
- **NIST CSF 2.0 – Protect Function (Awareness and Training category).**
- **DPDP Act 2023 Section 9(2)** – Mandate to prevent personal-data breach through reasonable safeguards.
- **ENISA 2025 Human Element Analysis** – Empirical data on user-originated incidents.

Indicative Evidence

- Annual training coverage and phishing-simulation participation rates.
- Specialized training for high-risk roles (administrators, DPOs, plant operators).
- Behavioural metrics: reporting rate of suspicious emails, quiz scores, incident reports raised by employees.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- Inclusion of privacy awareness in onboarding and vendor induction programs.

Interlinkages

Directly supports **Governance & Leadership**, **Identity & Access**, and **Privacy & Data Protection**. Improved culture metrics correlate with maturity in **Incident Response** due to faster detection and escalation by staff.

12. Monitoring & Detection

Definition

Monitoring & Detection establishes the telemetry, detections, and workflows that surface security/privacy-relevant events with enough fidelity and speed for action. It covers log/telemetry collection, detection engineering, alert triage/case handling, automation, and measurement of effectiveness.

Rationale

You can't respond to what you can't see. High-quality signals and tuned detections reduce noise, shorten mean time to detect/respond, and directly improve outcomes in Incident Readiness and Business Continuity.

Alignment

- **NIST CSF 2.0** - Detect (DE) Function (and interfaces with Identify/Protect/Respond)
- **ISO/IEC 27001:2022** - Annex A controls for logging and monitoring (no proprietary text quoted)
- **MITRE ATT&CK** - Technique coverage and detection mapping (as a reference model)

Core Capabilities

- **Logging & Telemetry Coverage** — Collect and retain the right logs (endpoint, identity, network, cloud, application, SaaS) with time sync, integrity, and retention commensurate to risk.
- **Detection Engineering & Use Cases** — Documented use cases mapped to threats/ATT&CK, with version-controlled rules, peer review, and test artifacts.
- **Threat Intel & Enrichment** — Curated sources (commercial/open/community); enrichment in pipeline (geolocation, reputation, asset/user context).
- **Alert Triage & Case Management** — Severity schema, escalation paths, case linkage to incidents, and closure quality checks.
- **EDR/NDR/Cloud Detection Coverage** — Sensor deployment targets, health monitoring, and gap closure plans.
- **Automation & Orchestration (SOAR/Playbooks)** — Approved auto-actions for low-risk routines; human-in-the-loop for higher-risk steps.
- **Effectiveness & Metrics** — MTTD/MTTR, true-positive rate, alert fatigue/noise ratios, backlog age, detection coverage by top risks.

Indicative Evidence

- Current telemetry coverage map and log retention settings
- Detection/use-case inventory with owners, tests, and last review dates
- Triage runbooks, case samples, and escalation/notification logs
- Sensor health dashboards (EDR/NDR/cloud) and gap closure tickets

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- SOAR playbooks and change approvals
- Quarterly metrics pack (MTTD/MTTR, TP/FP, backlog, coverage)

Interlinkages

Feeds **Incident Readiness** (alerting and case handoff) and informs **Governance & Leadership** (risk-based investment decisions). Works with **Identity & Access** (identity telemetry), **Infrastructure Security** (sensor placement), **Application & Product Security** (app logs), **Privacy & Data Protection** (privacy-relevant events), and **Supply-Chain Security** (vendor alerts).

Summary of the Twelve Domains

Together, these twelve pillars form a **comprehensive maturity lattice** through which Indian organizations can evaluate their current posture and plan targeted improvements. Each domain corresponds to measurable evidence categories in the NIRMATA Self-Assessment Workbook and links directly to regulatory and standard frameworks, ensuring that the assessment outputs are both **auditable** and **policy-aligned**. By assessing consistently across all twelve domains, an organization can progress methodically from **Level 0 (Unaware)** to **Level 5 (Resilient)** maturity—transforming fragmented compliance activity into structured, measurable trust.

The NIRMATA Maturity Model (Levels 0–5)

1. Purpose and Design

The **NIRMATA Maturity Model** defines six progressive levels—ranging from *non-existent* to *resilient*—that collectively represent the evolution of an organization's capability to manage information risk, privacy, and AI governance in measurable terms. It is designed to be **scalable, evidence-based, and auditable**, enabling both self-assessment and formal verification depending on the maturity tier achieved.

The model is structured around three design goals:

1. **Accessibility:** allowing all organizations, including MSMEs, to initiate structured self-assessments.
2. **Credibility:** establishing verification gates where independent validation is necessary for higher assurance levels.
3. **Consistency:** aligning maturity indicators with international frameworks such as **ISO/IEC 27001**, **ISO/IEC 27701**, **ISO/IEC 42001**, and **NIST CSF 2.0**, while remaining grounded in the **DPDP Act 2023** and **CERT-In Directions 2022**.

2. Assurance Model and Verification Logic

To balance inclusivity with integrity, NIRMATA adopts a **two-tier assurance structure**:

Maturity Level	Designation	Verification Mode	Description
Level 0 – Non-existent / Unaware	Foundational	**Self-declared**	Organization recognizes absence of structured controls. Used to establish baseline.
Level 1 – Initial / Reactive	Foundational	**Self-declared**	Activities occur in response to incidents; no formal governance or policy framework.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Level 2 – Defined / Emerging	Foundational	**Self-assessed**	Policies, procedures, and roles documented; limited adoption or enforcement.
Level 3 – Implemented / Managed	Foundational	**Self-assessed with internal validation**	Standardized, repeatable processes with evidence reviewed by internal audit or management.
Level 4 – Measured / Integrated	Verified	**Third-party verified** (e.g., Elytra Security, CERT-In empanelled auditor, or accredited audit firm)	Quantitative control measurement, automation, and evidence validated through external audit.
Level 5 – Resilient / Trusted	Verified	**Externally validated and peer-reviewed** (e.g., multi-auditor consortium or sectoral authority)	Continuous improvement demonstrated through verified metrics, transparency, and public disclosure.

This assurance model parallels practices under **ISO audit typology (First, Second, and Third Party Audits)** and **CMMI appraisal frameworks**, providing a clear and traceable maturity-to-assurance mapping.

3. Cross-Level Characterization

Level	Characterization	Organizational Behavior	Cultural Indicators	Typical Evidence
0 – Non-existent / Unaware	No formal awareness or assigned responsibility.	Reliance on vendor defaults; security and privacy not budgeted.	Indifference or lack of understanding of data responsibilities.	None or ad-hoc documents.
1 – Initial / Reactive	Awareness exists but practices are inconsistent.	Controls deployed reactively after incidents.	Compliance viewed as external imposition.	Isolated incident logs; unstructured actions.
2 – Defined / Emerging	Policies and roles exist; partial implementation.	Departmental procedures defined but siloed.	Growing understanding of governance value.	Policy manuals, partial risk registers.
3 – Implemented / Managed	Organization-wide processes standardized and monitored internally.	Management reviews performance; improvement projects initiated.	Shared accountability culture emerging.	Internal audit reports; metrics dashboards.
4 – Measured / Integrated	Quantitative metrics, automation, and cross-domain integration.	Data-driven decision-making; external verification.	Compliance embedded into operations.	Third-party audit reports; continuous monitoring metrics.
5 – Resilient / Trusted	Continuous improvement, transparency, and benchmarking.	Trust outcomes independently validated and published.	Culture of accountability and proactive adaptation.	Peer-reviewed reports; maturity certificate or

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Level	Characterization	Organizational Behavior	Cultural Indicators	Typical Evidence
				public declaration.

4. Detailed Level Descriptions

Level 0 – Non-existent / Unaware

Organizations at this stage have **no defined governance structure** for security or privacy.
Risk and incident management are informal or absent.
Awareness of obligations under the **DPDP Act 2023** and **CERT-In Directions 2022** is minimal.
This level forms the baseline for all subsequent improvement.

Indicators:

- Absence of dedicated security/privacy staff or budget.
- Unrecorded incidents and no systematic remediation.
- No data inventory or retention controls.

Level 1 – Initial / Reactive

Controls are ad-hoc, implemented only after adverse events.
Responsibilities are assigned informally, and awareness is limited to individual initiative.
Documentation, if present, lacks version control or approval.

Indicators:

- Incident responses depend on individual expertise.
- No central policy or repeatable process.
- Inconsistent regulatory compliance.
- Reactive culture; no preventive mindset.

Level 2 – Defined / Emerging

Policies, roles, and procedures have been established but are inconsistently applied.
Risk and compliance registers exist but may not cover all systems or business units.
Data classification, access control, and awareness programs are introduced but not yet institutionalized.

Indicators:

- Approved policy framework; partial training coverage.
- Evidence of risk registers or compliance logs.
- Privacy and incident plans drafted but untested.
- Emerging governance committees without clear accountability.

Level 3 – Implemented / Managed

At this level, the organization has standardized and documented processes that are routinely followed and internally audited.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

KPIs and KRIs are defined, and senior management regularly reviews results. Incidents are logged, analyzed, and tracked to closure.

Indicators:

- Regular internal audits; management review records.
- Evidence-based improvement actions.
- Integration of Privacy & Data Protection into ISMS.
- Cultural shift from compliance to ownership.

Verification Mode: *Self-assessment with internal validation.*

Level 4 – Measured / Integrated

Controls are quantitatively measured for effectiveness and integrated across departments. Automation supports monitoring, and metrics inform governance decisions. External audit or independent verification validates maturity claims.

Indicators:

- Control-effectiveness metrics and trend analysis.
- Integration of IT, OT, and privacy data in unified dashboards.
- Third-party verification of incident handling and recovery times.
- Demonstrated compliance with multiple frameworks (ISO 27001/27701/42001).

Verification Mode: *Third-party verified (Elytra Security, CERT-In empanelled auditor, or accredited firm).*

Level 5 – Resilient / Trusted

Organizations at this level exhibit **trust maturity as a strategic differentiator**. They operate continuous-improvement loops, engage in transparency reporting, and benchmark externally.
Resilience is engineered into processes, and leadership commitment is visible in board-level oversight.

Indicators:

- Predictive analytics for risk and anomaly detection.
- Independent peer review and publication of metrics.
- Cross-sector benchmarking participation (e.g., TRUST-IN Bharat index).
- Demonstrable stakeholder confidence and public trust indicators.

Verification Mode: *Externally validated and peer-reviewed.*

5. Transition Logic

Progression through maturity levels follows four transformation stages:

1. **Establish** – awareness, policy definition, and role assignment (Levels 0–1).
2. **Formalize** – documentation and basic process control (Level 2).

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

3. **Institutionalize** – standardization and internal validation (Level 3).
4. **Validate and Benchmark** – external verification and transparency (Levels 4–5).

Each transition requires both **quantitative improvement** (control performance) and **qualitative change** (governance behavior and culture).

6. Evidence Confidence Factor (ECF)

To ensure scoring integrity, NIRMATA introduces an **Evidence Confidence Factor (ECF)**—a numerical modifier (0.5–1.0) applied to each domain score based on verification strength:

Confidence Level	Evidence Source	Modifier
High	Independently verified by third party or regulator	1.0
Medium	Reviewed by internal audit or compliance team	0.8
Low	Self-declared without validation	0.5

Overall maturity is calculated as: **Weighted Domain Score × ECF**, ensuring that organizations relying solely on self-declaration cannot artificially inflate maturity ratings.

7. Outcome

The NIRMATA Maturity Model therefore provides both **a diagnostic pathway** for internal improvement and **a recognition mechanism** for verified excellence. By coupling self-assessment at Levels 0–3 with verified evaluation at Levels 4–5, it enables **broad adoption without diluting credibility**. This dual-assurance model allows independent auditors, CERT-In empanelled entities, or Elytra Security to serve as **Competent Authorities** under a voluntary national framework—paving the way for standardized, trusted maturity certification across India's digital economy.

6. Scoring and Interpretation Framework

6.1 Purpose and Overview

The **NIRMATA Scoring and Interpretation Framework** provides a transparent, reproducible method for translating qualitative self-assessment responses into a **quantitative maturity index (0 – 5)**. It enables organizations of any size or sector to:

- Evaluate their **current posture** across the twelve NIRMATA domains.
- Identify **gaps and improvement priorities**.
- Track **progress over time** using comparable metrics.
- Communicate results credibly to boards, regulators, and partners.

The framework is intentionally arithmetic and evidence-based. All calculations can be reproduced using a spreadsheet or automated within the forthcoming **TRUST-IN Portal**, ensuring that every maturity level corresponds to verifiable evidence.

6.2 The 0–5 Question Response Scale

Each question within the self-assessment is rated on a six-point scale from **0 (Not Implemented)** to **5 (Institutionalized)**. This refined model allows assessors to recognize incremental progress and prevents arbitrary "yes/no" rounding.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Score	Label	Definition — What It Represents	Typical Evidence
0	**Absent**	Control not implemented or unknown.	None; reliance on vendor defaults or informal practice.
1	**Initial**	Ad hoc, reactive, dependent on individuals.	Email instructions, corrective action log, vendor fix.
2	**Defined**	Policy or process exists but inconsistently applied.	Draft policies, approved implementation plan.
3	**Implemented**	Consistently executed and documented.	Pilot rollout, partial audit trail, limited training.
4	**Measured**	Monitored for performance and effectiveness.	Internal audits, KPIs, dashboards.
5	**Optimized**	Continually improved and integrated enterprise-wide.	ISO / CERT-In certificate, public transparency statement.

Evidence Expectation Matrix

Level	Documentation	Operation	Measurement	Validation
0	None	None	None	None
1	Informal	Ad-hoc	None	None
2	Draft	Planned	None	None
3	Formal	Partial	Occasional	Internal
4	Formal	Full	Regular	Internal + sample external
5	Public / Benchmarked	Continuous	Quantitative	External + peer benchmark

6.3 Evidence Confidence Factor (ECF)

Because maturity is inseparable from assurance, every domain's score is adjusted by an **Evidence Confidence Factor** that reflects how strongly the responses are validated.

Confidence Level	Definition	Typical Evidence	Multiplier
High (1.0)	Verified by an accredited third party or regulator.	ISO / CERT-In audit report, external assurance letter.	1.0
Medium (0.8)	Reviewed by internal audit or compliance committee.	Internal audit report, signed management review.	0.8
Low (0.5)	Self-declared without independent review.	Questionnaire responses, self-certification only.	0.5

Applying ECF ensures that two organizations with identical answers but different levels of verification do **not** receive identical maturity scores.

6.4 Domain Weighting

Each of the twelve domains contributes a specific percentage to the overall maturity score, reflecting its relative importance to the sector.
Weights sum to 100 %. The example below shows **Manufacturing Sector v1.1** calibration (derived from ENISA ETL 2025, DBIR 2025, and Dragos 2025).

Domain	Weight (%)	Rationale
Governance & Leadership	10	Required for oversight and DPDP/CERT-In accountability.
Risk & Compliance	20	Consolidates enterprise risk management and

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

		legal/contractual compliance (DPDP, CERT-In).
Asset & Data Management	8	High data-exposure risk; classification and retention underpin lawful, secure processing.
Identity & Access	8	Credentials/privilege remain top breach vectors; least privilege and strong auth reduce blast radius.
Infrastructure Security	12	Highest exposure and production criticality across IT/OT; includes Operational Technology & IoT Security.
Application & Product Security	6	Secure SDLC and software supply chain (SBOM/provenance); includes AI Governance & Ethical Use.
Supply-Chain Security	8	Third-party cascade risk; assurance and exit readiness limit impact.
Incident Readiness	4	Tested response, notification paths, and post-incident learning meet regulatory timelines.
Business Continuity & Resilience	4	RTO/RPO, backups/restores, and failover patterns ensure service restoration.
Privacy & Data Protection	6	DPDP obligations (consent, DPR, safeguards) and processor oversight.
Culture, Training & Awareness	8	Human factors drive incidents; role-based training and simulations improve outcomes.
Monitoring & Detection	6	Telemetry, tuned detections, and triage reduce MTTD/MTTR and improve IR effectiveness.

Sector baselines may be calibrated within guideline bands (typically ±2%) to maintain cross-industry comparability; **archetype-specific pilots (MSME/Mid/Large) may deviate further where risk profiles warrant**, with the rationale documented in the pilot plan.

6.5 Scoring Formulae

Let:

- **Qi** = Score (0–5) for each question within a domain.
- **n** = Number of applicable questions.
- **Wi** = Domain Weight (%).
- **ECF** = Evidence Confidence Factor (0.5 / 0.8 / 1.0).

Domain Score (Ds): $Ds = (\Sigma Qi) / n$

Weighted Domain Contribution (Wc): $Wc = (Ds / 5) \times Wi \times ECF$

Overall Maturity Level (OML): $OML = 5 \times (\Sigma Wc / 100)$

OML ranges from 0 to 5 and is mapped to qualitative classifications as shown in § 6.8.

6.6 Worked Example

Domain	Avg Score (0–5)	Weight (%)	ECF	Weighted Contribution
Governance & Leadership	4.00	10	0.8	6.40

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Domain	Avg Score (0–5)	Weight (%)	ECF	Weighted Contribution
Risk & Compliance	3.50	20	0.8	11.20
Asset & Data Management	3.00	8	0.8	3.84
Identity & Access	3.50	8	0.8	4.48
Infrastructure Security	2.80	12	0.8	5.38
Application & Product Security	2.50	6	0.5	1.50
Supply-Chain Security	3.20	8	0.8	4.10
Incident Readiness	3.00	4	0.8	1.92
Business Continuity & Resilience	2.70	4	0.8	1.73
Privacy & Data Protection	2.20	6	0.8	2.11
Culture, Training & Awareness	3.80	8	1.0	6.08
Monitoring & Detection	3.00	6	0.8	2.88
Total Weighted Contribution				51.61

Calculation: Weighted Pillar Contribution (Wp) = (Avg Score ÷ 5) × Weight × ECF

OML = 5 × (51.61 ÷ 100) = 2.58

Result: Overall Maturity Level = 2.58 → Level 2 (Defined)

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Interpretation: Policies and governance exist; implementation is uneven. Targeted improvements in Infrastructure, Privacy, and APS will lift overall maturity.

6.7 Visualization — The TRUST-IN Maturity Radar

The **Maturity Radar** depicts each domain's 0–5 score on a 12-axis chart. A circular shape indicates balanced maturity; dents highlight focus areas.

- **Spikes** → over-developed controls relative to peers.
- **Gaps** → domains below 3 require immediate attention.
- **Area under curve** ≈ overall resilience index.

Radar charts will be auto-generated in the Portal and included in organization reports.

6.8 Maturity Classification Matrix

Score Range (0–5)	Level	Descriptor	Verification Mode	Indicative State
0 – 0.9	0	Non-Existent / Unaware	None	No formal controls.
1.0 – 1.9	1	Initiated / Reactive	Self-declared	Ad-hoc response after incidents.
2.0 – 2.9	2	Defined / Emerging	Self-assessed	Policies documented; partial implementation.
3.0 – 3.9	3	Implemented / Managed	Internally validated	Standardized, reviewed controls.
4.0 – 4.5	4	Measured / Integrated	Third-party verified	Quantified performance and automation.
4.6 – 5.0	5	Resilient / Trusted	Certified / Peer-reviewed	Continuous improvement and public transparency.

Levels 0 – 3 are self-certifiable; Levels 4 – 5 require independent verification by a competent authority (Elytra Security, CERT-In empanelled auditor, or accredited body).

6.9 Example Executive Summary Output

Attribute	Illustrative Output
Organization	ABC Manufacturing Pvt Ltd
Sector	Automotive Manufacturing
Assessment Type	Self-Assessment (Internal Audit Validated)
Overall Maturity Level	**2.73 — Defined / Emerging**
Highest Domain	Governance & Leadership (4.0)
Lowest Domain	Privacy & Data Protection (2.0)
Key Improvement Areas	OT Security, Privacy & Data Protection
Average Confidence Factor	0.76
Target Next Year	Level 3.5 — Implemented / Managed

6.10 Transparency and Reproducibility

All formulas, weightings, and confidence definitions are published under **Creative Commons BY-SA 4.0**.
Any organization can reproduce calculations independently or audit another entity's results

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

using identical parameters.
This open-methodology approach ensures:

- **Credibility** — every figure traceable to evidence.
- **Consistency** — identical scoring nationwide.
- **Comparability** — cross-sector benchmarks possible.

6.11 Summary

The **NIRMATA Scoring and Interpretation Framework** transforms complex governance and security maturity into an **objective, evidence-anchored metric**. It supports both entry-level awareness (Levels 0–2) and world-class resilience (Levels 4–5). By combining a refined 0–5 response scale, evidence confidence factors, and sector-specific weighting, it provides a single, nationally consistent language for trust measurement in India's digital economy.

7. Sectoral Calibration — Manufacturing Pilot Model (MSME, Mid-Size, Large)

7.1 Why Manufacturing first

- **Attack pressure is high and rising:** Global threat reporting ranks **ransomware, supply-chain compromise, and phishing** among the top disruption drivers. ENISA Threat Landscape 2025 analyzes 4,875 incidents (Jul 2024–Jun 2025) and lists those as the dominant production-sector attack modes.
- **Manufacturing remains a primary target:** IBM X-Force 2025 identifies manufacturing as the **most targeted industry**, with exploitation of public-facing apps and credential harvesting as key entry points.
- **Ransomware impact:** Dragos 2025 logs 1,693 industrial ransomware attacks (≈ 87 % YoY increase), manufacturing hardest hit.
- **Human factor:** Verizon DBIR 2025 shows phishing + credential misuse still dominate breaches; SMBs mirror this trend.

Indian context: CERT-In Directions 2022 (6-hour reporting, log retention, time sync) and the **DPDP Act 2023** (consent, notice, grievance duties) apply to factories handling employee or supplier personal data.

Programme goal: Raise MSME resilience — the foundation of India's industrial economy — while scaling guidance for mid-size and large enterprises.

7.2 Threat landscape for plant leaders (plain language)

- **People are the first line:** Most intrusions start with phishing or credential reuse; MFA + awareness training mitigate most.
- **OT is now a target:** Legacy PLCs/SCADA and remote OEM access create side doors; segment IT–OT and log connections.
- **Suppliers matter:** A weak vendor can infect the plant; insert security/privacy clauses and review annually.
- **Controls must work:** Picus Blue 2025 finds avg. preventive efficacy ≈ 69 % — validate regularly.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

7.3 Three calibrated archetypes

Reading the tables

Weights sum to 100 %. They reflect risk and resource reality. Evidence and quick wins are phrased for non-technical owners.

A. MSME Manufacturer (Founder-led; ≤ 300 staff)

Domain	Weight %	Plain-language rationale
Culture & Awareness	**12**	Human factor dominates breaches (DBIR 2025).
Access & Identity	**10**	MFA and user cleanup stop credential abuse.
Operational Technology & IoT Security	**12**	Remote OEM links are risk points.
Incident Readiness	**10**	Six-hour CERT-In rule needs plan.
Privacy & Data Protection	**9**	DPDP grievance + notice compliance.
Vendor & Supply Chain	**9**	Supplier weakness common.
Data Lifecycle	8	Retain only needed records.
Governance & Leadership	8	Assign a named owner.
Risk Management	7	Maintain one risk log.
Compliance Mgmt	6	Minimal legal recordkeeping.
Metrics & Improvement	5	Few KPIs monthly.
AI Governance	4	Low relevance today.
Total	**100**	

Evidence Examples: MFA enabled; training records; simple network sketch; privacy notice; incident contact sheet.
90-day wins: (1) MFA on email & VPN (2) Phishing drill (3) OEM access rules (4) Privacy inbox (5) CERT-In contact.

B. Mid-Size Manufacturer (500–2 000 staff)

Domain	Weight %	Rationale
Operational Technology & IoT Security	**14**	Multiple plants, OEM VPNs.
Incident Readiness	**12**	Downtime = ₹ loss.
Culture & Awareness	**10**	Contractor rotation needs training.
Access & Identity	**9**	Privileged Access Mgmt.
Vendor & Supply Chain	**9**	Dozens of partners.
Data Lifecycle	8	IP drawings + DLP.
Privacy Ops	8	DPIA, grievances.
Governance	7	Board oversight.
Risk Mgmt	7	Enterprise risk register.
Compliance	6	CERT-In reporting.
Metrics & Improve	5	KPI tracking.
AI Governance	5	ML in QC.
Total	**100**	

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Evidence: OT inventory; VPN MFA; quarterly drills; DPO dashboard; vendor checklist; phishing stats.
Quick wins: Segment IT/OT; two tabletops; privacy notice + DSR SLA; admin rights review.

C. Large Industrial Enterprise (≥ 2 000 staff)

Domain	Weight %	Rationale
Operational Technology & IoT Security	**15**	Legacy + modern mix.
Incident Readiness	**12**	Cross-plant continuity.
Vendor & Supply Chain	**10**	Hundreds of processors.
Access & Identity	**9**	Federation / Zero Trust.
Culture & Awareness	**9**	Scale → behavior analytics.
Privacy Ops	8	DPDP + cross-border.
Data Lifecycle	8	IP retention.
Risk Mgmt	7	Quantified KRIs.
Governance	7	KPIs → Board.
Compliance	6	Multi-regulatory.
Metrics & Improve	5	Continuous validation.
AI Governance	4	Model inventory + drift.
Total	**100**	

Evidence: IEC 62443 baselines; red/blue/purple tests; vendor attestations; ISO certs; AI bias testing.
Quick wins: Broker all OEM links; central IAM; top 25 vendor attestations; privacy notice for visitors.

7.4 Comparative summary

- **MSME:** People & privacy first.
- **Mid-Size:** Operational readiness and vendor assurance.
- **Large:** Integrated OT and supply-chain governance with quantitative metrics. Trendlines mirror global evidence that human error + ransomware + supply-chain form the dominant risk triad.

7.5 How to run a pilot (non-technical)

1. Appoint a responsible person (plant head or HR).
2. Collect basic evidence in one folder.
3. Use the 0–5 response scale (Section 6A).
4. Attach one proof per question (screenshot / PDF / photo).
5. Review the radar and select top 5 actions (3 people + 2 technical).
6. Re-assess after 90 days → habit formation.

7.6 Illustrative MSME progress (after 90 days)

Domain	Before	After	Note
Culture	2	3	Phishing drill + training done
Access	1	3	MFA + user cleanup

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Privacy	1	2	Notice + inbox
OT	1	2	OEM session control
IR	0	2	CERT-In plan posted

Overall: +0.5 to +0.8 on OML — often a full band jump.

7.7 DPDP & CERT-In checklist for plants

- **DPDP Act 2023:** Display notice; record lawful basis; grievance inbox; close requests ≤ 30 days.
- **CERT-In 2022:** Report within 6 h; retain logs 180 days; sync system time; keep contacts handy.

7.8 Evidence maturity ladder (by size)

Area	MSME	Mid-Size	Large
Identity	MFA + monthly review	PAM + quarterly recert	IAM + JIT/JEA + SSO
OT	Sketch + OEM rules	VLAN + logs	IEC 62443 baseline + broker
Culture	E-module + drill	Role modules + quarter drill	Analytics + coaching
IR/BC	1-page plan	Playbooks + tabletop	Cross-plant exercises
Privacy	HR notice + inbox	DPIA + tracking	PIMS + cross-border controls
Metrics	5 KPIs	Dashboards + purple team	Continuous validation

7.9 Verification levels (4–5)

- **0–3: Self-certified; build habits and evidence.**
- **4–5: Independent audit required (CERT-In empanelled / Elytra Security).**
- Continuous validation essential — Picus Blue 2025 shows average control efficacy < 70 %.

7.10 Policy and association insights

- MSME uplift needs ready-made templates + short courses.
- Associations can host 90-day cohorts to create peer pressure and shared learning.
- Pilot data (anonymous) feeds a national "State of Trust in Bharat" index to guide future DPDP rules and CERT-In updates.

Key references used

ENISA ETL 2025 ; Verizon DBIR 2025 ; IBM X-Force 2025 ; Dragos 2025 ; Picus Blue 2025 ; CERT-In 2022 ; DPDP Act 2023 .

8. Governance and Stewardship Framework

8.1 Purpose

The credibility of a national maturity framework depends not only on its technical quality but on **transparent governance, impartial verification, and predictable**

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

maintenance.
This section defines the stewardship model for the **NIRMATA Framework** and the **TRUST-IN Bharat Programme**.

8.2 Roles and Responsibilities

Entity / Role	Core Responsibility	Outputs / Deliverables
Custodian – Elytra Security	Framework design, research, publication, and maintenance.	Whitepaper, workbook, portal, annual "State of Trust in Bharat" report.
Verifiers / Assessors	Independent third parties (CERT-In empanelled auditors, accredited consulting firms, Elytra-approved partners).	Level 4–5 verification reports, evidence review statements.
Adopting Organizations	Conduct self-assessments (Levels 0–3), maintain evidence, and participate in pilots.	Assessment workbook, evidence pack, improvement plan.
Sector Associations (CII, FICCI, NASSCOM, Manufacturers' Chambers)	Dissemination, cohort training, feedback collection.	Sector adaptation notes, anonymized benchmark data.
Government Stakeholders (MeitY, BIS LITD 27, CERT-In)	Policy alignment, recognition, and integration with national standards.	Endorsement statements, policy advisories.
Academic and Research Partners	Peer review and empirical validation of scoring models.	Technical papers, pilot data analysis.

8.3 Governance Structure

```
Stewardship Board (Elytra Security)
 ├── Technical Standards Committee (Domain Experts)
 ├── Sector Advisory Councils (Manufacturing, BFSI, Healthcare, etc.)
 ├── Verification & Ethics Panel (Accreditation, Conflict-of-Interest)
 └── Secretariat (Publication, Portal Administration)
```

a. Stewardship Board

Oversees strategic direction, approves revisions, and coordinates with government bodies.

b. Technical Standards Committee

Maintains cross-walks with ISO 27001, 27701, 42001; NIST CSF 2.0; and updates domain indicators.

c. Sector Advisory Councils

Ensure contextual calibration and sector-specific guidance (manufacturing pilot, etc.).

d. Verification & Ethics Panel

Approves assessor accreditation criteria and enforces conflict-of-interest and independence rules.

e. Secretariat

Manages publications, stakeholder consultations, and open data repository (scores + trends, anonymized).

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

8.4 Framework Maintenance and Versioning

Activity	Frequency	Responsibility
Minor Revision (question updates, weight adjustments)	Annual	Technical Standards Committee
Major Revision (new domains, scoring logic)	Every 3 years	Stewardship Board + peer review
Public Comment Period	60 days before release	Secretariat
Publication	DOI + ISBN release on trustin.elytrasecurity.com	Secretariat
License	Creative Commons Attribution-ShareAlike 4.0 (CC BY-SA 4.0)	Custodian

All revisions are version-controlled (e.g., NIRMATA v1.0 → v1.1) and archived for historical reference.

8.5 Verification and Accreditation Model

8.5.1 Assurance Levels

Assessment Level	Who Performs It	Evidence Requirement	Output
Levels 0–3 (Self-Certification)	Organization's internal team (CISO, DPO, Plant Head).	Self-declared workbook + internal review notes.	Internal scorecard + action plan.
Level 4 (Third-Party Verified)	CERT-In empanelled auditor / Elytra-approved verifier.	Full evidence sampling + interviews + control tests.	Verified Maturity Report + certificate (valid 2 years).
Level 5 (Peer-Reviewed / Certified)	Independent panel drawn from the Verification & Ethics registry.	End-to-end audit + external benchmarking + public disclosure review.	NIRMATA Resilient Trust Certificate + benchmark listing.

8.5.2 Accreditation Principles

1. **Independence:** Assessors must have no commercial relationship with the assessed entity.
2. **Competence:** At least one lead assessor must hold ISO 27001 Lead Auditor or equivalent certification.
3. **Transparency:** All verifiers publish annual summary statistics (number of assessments, common findings).
4. **Rotation:** No verifier may audit the same organization more than twice consecutively.

8.6 Ethical and Transparency Principles

- **Open Methodology:** All scoring logic and weightings published under CC BY-SA 4.0.
- **Non-Commercial Access:** Core framework and workbook remain free for all Indian organizations.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- **Data Minimization:** Only anonymized metrics collected for national trend analysis.
- **Conflict of Interest Declaration:** Required from every assessor and peer reviewer.
- **Public Accountability:** Annual "State of Trust in Bharat" report summarizing sectoral progress, anonymized statistics, and improvement recommendations.

8.7 Coordination with National Standards Bodies

- **Bureau of Indian Standards (BIS LITD 27):** Liaison for possible national adoption or annex reference within emerging data-protection and AI-governance standards.
- **MeitY / CERT-In:** Alignment with DPDP Rules 2023 and CERT-In Directions 2022 to ensure legal interoperability.
- **State IT Departments:** Encourage translation and MSME outreach in regional languages.
- **International Engagement:** Exchange with NIST, ENISA, and ISO committees for harmonization and benchmarking.

8.8 Publication and Communication Cadence

Deliverable	Periodicity	Intended Audience
NIRMATA Framework Whitepaper (vX.Y)	Annual (July)	Industry + Regulators
Self-Assessment Workbook Update	Annual (Q3)	Organizations / Assessors
State of Trust in Bharat Report	Annual (Dec)	Public / Media / Policy
Peer-Review Journal / Case Studies	Continuous	Academia
Stakeholder Consultation Workshops	Twice a year	Sector Associations + Regulators

8.9 Custodian Statement

Elytra Security acts as the founding custodian of the NIRMATA Framework and TRUST-IN Bharat Programme.
It commits to maintaining the framework as a **public-interest, open-access initiative**, ensuring:

- neutrality and non-commercial governance;
- integration with national policy goals (Digital India, Cyber Surakshit Bharat);
- continual peer review by qualified experts; and
- open feedback channels for citizens and enterprises.

8.10 Summary

The governance framework ensures that NIRMATA remains **credible, inclusive, and sustainable**—
owned by India's community of practitioners, not by any single entity. Through open publication, independent verification, and transparent stewardship, **TRUST-IN Bharat** becomes not just a self-assessment tool, but a **national trust-infrastructure** that grows stronger with every participant.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

9. Implementation Roadmap and National Adoption Pathway

9.1 Objective

This section outlines how the **NIRMATA Framework** and **TRUST-IN Bharat Programme** will transition from concept to nationwide adoption. The roadmap ensures that implementation is **phased, evidence-driven, and inclusive**, reaching India's MSMEs as effectively as its large enterprises.

9.2 Guiding Principles

1. **Start Simple, Scale Fast:** Launch with a minimal viable toolkit (whitepaper + workbook + portal) and expand features iteratively.
2. **Inclusive by Design:** MSMEs receive templates, translated materials, and assisted onboarding.
3. **Evidence over Assertion:** Every maturity score supported by verifiable documentation.
4. **Voluntary, Not Punitive:** Participation builds readiness for regulation, not regulatory exposure.
5. **Public–Private Partnership:** Government recognition balanced by industry stewardship.
6. **Open-Source Ethos:** All scoring logic and datasets remain free and transparent.

9.3 Phased Implementation Plan (2025 – 2028)

Phase	Period	Focus Area	Key Deliverables	Lead / Partners
Phase 1 — Foundation (2025)	Q2 – Q4 2025	Establish baseline and pilots.	• Publish NIRMATA v1.0 Whitepaper & Workbook • Launch TRUST-IN Portal (pilot release) • Manufacturing MSME pilot (50 plants) • Training of Assessors Cohort 1 (100 participants)	Elytra Security + CII/FICCI + MeitY
Phase 2 — Scale-Up (2026)	Q1 – Q4 2026	Expand across sectors and languages.	• Add BFSI & Healthcare modules • Regional language toolkits (5 languages) • State MSME outreach with SIDBI & MSME Ministry • Launch annual	Elytra Security + State IT Depts + MSME Ministry

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Phase	Period	Focus Area	Key Deliverables	Lead / Partners
			"State of Trust in Bharat 2026" report	
Phase 3 — Verification Ecosystem (2027)	Q1 – Q4 2027	Formalize assessor accreditation.	• Release Assessor Accreditation Scheme • Launch Level 4–5 verification pilots • Create open-benchmark dashboard (anonymized data)	Elytra Security + CERT-In + BIS LITD 27
Phase 4 — National Recognition (2028)	Q1 – Q4 2028	Institutionalize NIRMATA as reference model.	• Submit proposal for BIS recognition / annex inclusion • Align with DPDP Rules and AI Regulation drafts • Publish NIRMATA v2.0 based on pilot evidence • Formal public benchmark portal and open data API	Elytra Security + MeitY + BIS + Industry Associations

9.4 Key Components of Implementation

a. Whitepaper & Workbook Publication

- **Whitepaper:** Baseline specification, versioned annually with DOI + ISBN.
- **Workbook:** Self-assessment spreadsheet + guide for each sector, updated yearly.

b. TRUST-IN Portal (Digital Platform)

Core digital interface where organizations:

- Register and perform online self-assessment.
- Upload limited evidence files (for verified levels).
- Visualize radar charts and download reports.
- Access anonymized benchmarks and improvement toolkits.

Phase 1 Portal Features

- Secure registration, sector tagging, and auto-scoring engine.
- Offline Excel import / export.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- English interface + Hindi and Tamil in Q4 2025.
- Privacy-by-design architecture (data stored in India).

Phase 2 Enhancements

- Multi-language expansion (> 8 languages).
- Verifier module for Levels 4–5.
- API integration with industry associations and government dashboards.

9.5 Pilot Execution Framework

a. Pilot Objectives

1. Validate the 0–5 scoring and evidence model in real settings.
2. Test usability among non-technical MSME owners.
3. Collect sector-wise risk and control effectiveness data.
4. Calibrate domain weights and question clarity.

b. Pilot Governance

- **Lead Coordinator:** Elytra Security (Framework Custodian).
- **Sector Mentor:** CII Manufacturing Panel.
- **Academic Observer:** IIT Madras / IIM Bangalore faculty for data validation.
- **Government Observer:** MeitY / CERT-In representative.

c. Pilot Cohorts

Cohort	Size	Region	Focus
MSME Cohort 1	50 plants	Maharashtra, Tamil Nadu, Gujarat	Baseline readiness
MSME Cohort 2	75 plants	Punjab, Haryana, UP	DPDP compliance + culture
Mid-Size Cohort 1	20 enterprises	PAN-India	OT + Supply-Chain focus
Large Enterprise Cohort 1	10 enterprises	PAN-India	Verification pilot (Level 4–5)

9.6 Stakeholder Engagement and Communication

Stakeholder	Engagement Channel	Purpose
MSMEs	Local industry clusters & chambers	Awareness sessions & tool training
Industry Associations	CII / FICCI / NASSCOM	Pilot coordination & feedback
Academia	IIT / IIM / NIT network	Research validation & metrics analysis
Government Agencies	MeitY / BIS / MSME Ministry	Recognition & policy alignment
Media & Public	Annual report & portal	Transparency & trust awareness

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

	dashboard	

9.7 Measurement of Success (KPIs)

Dimension	Key Metric	Target by 2028
Reach	Organizations registered on Portal	10 000 +
Coverage	Sectors with calibrated models	≥ 6
Capability	Certified Assessors trained	500 +
Improvement	Avg. maturity gain after 1 year	≥ +0.6 on 0–5 scale
Verification	Level 4–5 audits completed	200 +
Transparency	Annual reports published on time	100 % compliance

9.8 Risk and Mitigation Plan

Potential Risk	Impact	Mitigation Strategy
Low MSME adoption	Limits national reach	Partner with State MSME Depts + subsidize training
Assessor capacity constraints	Delays verification	Early accreditation drive + online training modules
Data privacy concerns	Participation hesitation	Minimal data collection + full transparency policy
Fragmented communication	Confusion in industry	Unified brand (TRUST-IN Bharat) + consistent messaging
Funding limitations	Slower expansion	PPP model + CSR & grant channels

9.9 Policy Recognition Pathway

a. Alignment with BIS & MeitY

- Engage **BIS LITD 27** to reference NIRMATA within forthcoming national standards on data security and AI governance.
- Submit framework for **BIS Technical Reference Document** status by 2028.
- Collaborate with **MeitY** to integrate TRUST-IN scores as voluntary readiness indicators for DPDP compliance.

b. Alignment with CERT-In

- Map NIRMATA domains to CERT-In reportable incident types and 6-hour response window.
- Develop joint training modules for MSMEs.

c. Integration with ESG and Corporate Disclosure

- Encourage listed companies to include TRUST-IN maturity scores in annual sustainability or ESG disclosures.
- Facilitate recognition under BSE/NSE ESG indices.

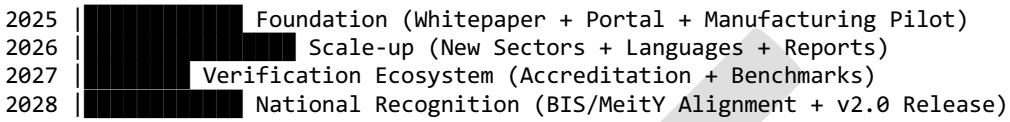
9.10 Sustainability and Funding

- **Public-Interest Model:** Core content free to use; revenues (if any) only from certification and training to sustain operations.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- **CSR and Grant Funding:** Leverage Digital India, Cyber Surakshit Bharat, and international cyber-capacity-building funds.
- **Academic Partnerships:** Encourage PhD/MTech projects using anonymized data for continuous research.
- **Open API Ecosystem:** Allow integration with state and industry dashboards without data duplication.

9.11 Indicative Timeline Chart (2025 – 2028)



9.12 Summary

By 2028, TRUST-IN Bharat will evolve from a sectoral pilot into a national benchmark for data security, privacy, and AI governance maturity.
Its success depends on collaboration: government for recognition, industry for execution, academia for evidence, and MSMEs for grass-roots adoption.

Through this roadmap, NIRMATA creates a clear path from self-awareness to national trustworthiness — turning India's industrial resilience into a measurable, auditable, and globally recognized strength.

10. References and Annexes

10.1 Reference Methodology

All citations used within the **NIRMATA Framework Whitepaper (v1.0)** originate from publicly available, peer-reviewed, or officially published sources.
Each report was reviewed between **July 2024 and February 2025** to ensure relevance, factual consistency, and alignment with the Indian regulatory environment.

Only **verified primary publications** are included; no derivative summaries, news articles, or secondary blogs have been used.
Where exact line citations appear in text, those correspond to document versions published by the issuing body in 2025.

10.2 Primary Global References

Ref. ID	Source	Title / Description	Publisher / Year	Relevance to NIRMATA Domains
[R1]	**ENISA Threat Landscape 2025 (ETL 2025)**	Annual analysis of European and global cyber threats.	ENISA, July 2025	Threat mapping, sectoral targeting, human factor risk (Domains 2, 6, 10).
[R2]	**Verizon Data Breach Investigations Report (DBIR) 2025**	Empirical global dataset of >30,000 incidents.	Verizon, 2025	Attack vectors, phishing prevalence, human error metrics (Domains 5, 10).
[R3]	**IBM X-Force Threat Intelligence Index 2025**	Annual threat trends, including India-specific incidents.	IBM, Feb 2025	Ransomware, credential misuse, manufacturing attacks (Domains 6,

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Ref. ID	Source	Title / Description	Publisher / Year	Relevance to NIRMATA Domains
				8).
[R4]	**Dragos Industrial Ransomware Report 2025**	Industrial and OT-specific incident analysis.	Dragos, Jan 2025	OT/IoT resilience, segmentation guidance (Domain 6).
[R5]	**Picus Security "Blue Report 2025"**	Control validation and mitigation effectiveness study.	Picus Labs, Mar 2025	Validation, simulation, and control efficacy metrics (Domain 11).
[R6]	**NIST Cybersecurity Framework 2.0 (CSF 2.0)**	Core functions, categories, and implementation tiers.	NIST, Feb 2024	Alignment basis for NIRMATA domains and levels (Governance, Risk, Metrics).
[R7]	**ISO/IEC 27001:2022**	Information Security Management Systems (ISMS).	ISO, 2022	Structural benchmark for Domains 1–4, 7, 8.
[R8]	**ISO/IEC 27701:2019**	Privacy Information Management System (PIMS).	ISO, 2019	Privacy & Data Protection and governance (Domain 9).
[R9]	**ISO/IEC 42001:2023**	Artificial Intelligence Management Systems (AIMS).	ISO, 2023	AI Governance and Ethical Use (Domain 12).
[R10]	**CMMI v2.0**	Capability Maturity Model Integration reference.	CMMI Institute, 2023	Conceptual basis for NIRMATA maturity levels.

10.3 Indian Legal and Regulatory References

Ref. ID	Instrument / Standard	Issuing Authority / Date	Relevance
[I1]	**Digital Personal Data Protection Act 2023 (DPDP Act)**	Ministry of Electronics and IT (MeitY), Aug 2023	Lawful processing, notice, consent, grievance, retention.
[I2]	**CERT-In Directions under Section 70B(6) of the IT Act**	Indian Computer Emergency Response Team, Apr 2022	Mandatory incident reporting, log retention, and time synchronization.
[I3]	**Cyber Security in Power Sector Guidelines**	Ministry of Power, 2021	Sectoral OT security model for adaptation.
[I4]	**National Cyber Security Policy Draft 2023 (MeitY)**	Government of India	Strategic context for national resilience.
[I5]	**BIS LITD 27 / ISO IEC JTC 1 Mirror Committee Records**	Bureau of Indian Standards	Governance linkage for formal adoption and liaison.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

10.4 Secondary Guidance and Analytical References

Ref. ID	Source	Purpose / Usage in Framework
[S1]	**World Economic Forum – Global Cybersecurity Outlook 2025**	Context for risk prioritization and C-suite awareness.
[S2]	**OECD AI Risk Management Framework 2024**	Comparative mapping for Domain 12 (AI Governance).
[S3]	**ENISA Cybersecurity Skills Framework 2024**	Alignment for workforce and awareness metrics.
[S4]	**NIST SP 800-61 r3 (Computer Security Incident Handling Guide)**	Guidance on incident response processes.
[S5]	**NIST SP 800-82 r3 (Guide to Industrial Control Systems Security)**	Basis for OT/IoT controls.

10.5 Cross-Reference Table (Framework Alignment)

NIRMATA Domain	Primary Global Reference(s)	Indian Law / Rule
Governance & Leadership	ISO 27001 cl. 5 & 7	DPDP s. 10(2)(a)
Risk Management	NIST CSF Identify (ID.RA)	CERT-In Direction 2
Compliance Management	ISO 27001 cl. 9 & 10	DPDP Rule 8 (draft)
Data Lifecycle & Classification	ISO 27001 A.5.12–A.5.13	DPDP s. 8 (2)
Identity & Access	NIST CSF Protect (PR.AC)	CERT-In Direction 6
Operational Technology & IoT Security	NIST SP 800-82 r3	Power Sector Guidelines 2021
Vendor & Supply Chain	ENISA ETL 2025 (Chapter 5)	DPDP s. 8 (7)
Incident Readiness	NIST SP 800-61 r3	CERT-In Direction 1
Privacy & Data Protection	ISO 27701 cl. 6 & 7	DPDP s. 9–11
Culture & Workforce Awareness	ENISA Skills Framework 2024	MeitY Cyber Awareness Programme
Metrics, Monitoring & Improvement	Picus Blue 2025 + NIST CSF 2.0 (Detect)	CERT-In Direction 3
AI Governance & Ethical Use	ISO 42001 + OECD AI RMF	DPDP s. 10 + AI Policy Draft 2024

10.6 Annex Summaries

Annex	Title	Contents
Annex A	*Detailed Domain-Level Indicators (0–5)*	Full ladder for each of the twelve domains, aligned with scoring logic in Section 6.
Annex B	*Manufacturing Pilot Data Collection Template*	MSME, mid-size, and large enterprise data-capture format used during pilot phase.
Annex C	*Assessor Accreditation Guidelines (Levels 4–5)*	Eligibility criteria, code of conduct, and verification checklist.
Annex D	*Sample Radar Visualization and Interpretation Guide*	Visual reference for portal reporting and annual benchmarking.
Annex E	*Cross-Framework Concordance Matrix*	Comparative mapping of NIRMATA ↔ ISO ↔ NIST ↔ DPDP ↔ CERT-In ↔ AI Governance.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

10.7 Citation Format

Preferred citation for academic or industry references:

Elytra Security (2025). *TRUST-IN Bharat — The NIRMATA Framework: National Information Risk Maturity and Trust Assessment v1.0.* DOI 10.5281/trustin-nirmata-2025. Licensed CC BY-SA 4.0. Available at https://elytrasecurity.com/trustin

10.8 Closing Note

This reference corpus forms the **empirical and normative foundation** of NIRMATA v1.0.
It ensures that every maturity criterion, weighting, and recommendation is grounded in verifiable evidence and contemporary law.
Future editions will continue to align with **updated ENISA, NIST, ISO, and Indian statutory releases** to preserve both international compatibility and national sovereignty in cybersecurity and privacy governance.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Annex A — Domain-level Maturity Indicators (0–5)

NIRMATA Framework v1.0

Each NIRMATA domain follows the same six-level maturity scale. The indicators below show observable characteristics and typical evidence at each level. Organizations should assess themselves **per domain**, not by averaging across the enterprise.

How to read this annex

Each pillar has six maturity levels (0–5). "Characteristics" describe observable practices; "Indicative Evidence" lists common artifacts reviewers look for. Use these as guidance; do not treat them as certification criteria.

1. Governance & Leadership

Level	Characteristics	Indicative Evidence
0	No defined governance for security/privacy/AI; ad-hoc ownership.	No charters; no named roles; no budget lines.
1	Policies exist but informal; responsibilities unclear; limited oversight cadence.	Draft policy docs; sporadic meeting notes.
2	Named owners (CISO/DPO); annual objectives; basic risk reporting to management.	Role letters; annual plan; risk dashboard sample.
3	Board/committee oversight; KPIs/KRIs tracked; funding linked to risk.	Committee minutes; approved budget; KPI pack.
4	Enterprise governance playbooks; independent reviews; cross-pillar coordination.	Playbooks; internal audit/assurance reports.
5	Outcomes-based governance with continuous improvement and transparency where appropriate.	Management review outputs; trend analyses.

2. Risk & Compliance

Level	Characteristics	Indicative Evidence
0	No risk register; obligations unknown; audits ad-hoc.	—
1	Basic asset/risk lists; obligations tracked informally.	Sheets/emails; scattered findings.
2	Methodology defined; periodic assessments; mapped obligations.	Risk method; register; compliance matrix.
3	Treatment plans with owners/dates; testing program; exceptions managed.	Risk treatment logs; control tests; exceptions.
4	Quantified/business-linked risks; regulatory notifications workflow; control assurance.	Loss scenarios; regulator logs; assurance reports.
5	Integrated GRC across IT/OT/AI; risk appetite and metrics drive investment.	Appetite statements; heatmaps with trends.

3. Application & Product Security (includes AI Governance & Ethical Use)

Level	Characteristics	Indicative Evidence
0	No secure development practices; direct production changes; unknown dependencies.	—
1	Fixes after incidents; third-party code used without review.	Email fixes; ad-hoc notes.
2	Secure SDLC policy drafted; basic SAST/SCA pilots;	Policy drafts; pilot

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Level	Characteristics	Indicative Evidence
	SBOM concept.	reports.
3	Standardized SDLC; SAST/SCA in CI; basic DAST; secrets managed; SBOM for releases; app logs defined.	CI logs; SBOM files; release gates.
4	Signed builds/provenance; gated CI/CD; API security patterns; IaC scanning; periodic pen tests; app logs feed Monitoring & Detection.	Build attestations; gateway policies; pen-test reports.
5	Threat modeling embedded; bug bounty/purple-team; measurable defect/leakage reduction; AI controls integrated.	TM artifacts; bounty reports; trend dashboards.

4. Asset & Data Management

Level	Characteristics	Indicative Evidence
0	Unknown data locations; no classification/retention.	—
1	Basic inventories; informal retention.	Spreadsheets; ad-hoc deletes.
2	Classification scheme; retention policy; initial encryption/DLP baselines.	Approved schemas; policy; config baselines.
3	Data flows mapped; retention enforced; periodic deletion/anonymization; access tied to classification.	Flow diagrams; job logs; access reviews.
4	Automated discovery/labeling; lifecycle controls across apps/SaaS; regular policy attestation.	Discovery scans; DLP events; attestations.
5	Business-aligned data minimization; continuous validation; measurable reduction in sensitive data exposure.	Trend metrics; minimization evidence.

5. Identity & Access

Level	Characteristics	Indicative Evidence
0	Shared/admin accounts; weak auth; no reviews.	—
1	Some MFA for IT; manual provisioning; sporadic reviews.	MFA list; emails.
2	RBAC defined; JML workflow; MFA for privileged users; initial PAM.	RBAC matrix; JML tickets; PAM config.
3	MFA for all feasible users; periodic access reviews; break-glass controls; service account governance.	Review records; SoD analysis.
4	Conditional access; least-privilege by design; identity telemetry to Monitoring & Detection.	Policies; telemetry dashboards.
5	Risk-adaptive access; continuous verification; secrets rotation/zero-trust patterns across environments.	Policy-as-code; rotation logs.

6. Infrastructure Security (includes Operational Technology & IoT Security)

Level	Characteristics	Indicative Evidence
0	Flat networks; unpatched systems; unreliable backups.	—
1	Baseline firewalls; reactive patching; OEM remote access unmanaged.	Change emails.
2	Inventories (IT + key OT); segmentation plan; backup/restore plan; scan pilots.	Inventories; VLAN/zone plan; backup plan.
3	Hardened builds; enforced IT/OT segmentation; EDR on IT; controlled OEM access; tested restores (samples).	Baselines; diagrams; EDR console; restore

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Level	Characteristics	Indicative Evidence
		reports.
4	NDR/flow monitoring; config compliance; OT aligned with IEC 62443 where applicable; firmware change control.	NDR dashboards; drift reports; change records.
5	Zero-trust patterns; continuous control validation; integrated IT/OT monitoring; measured blast-radius and recovery improvements.	Micro-seg; validation results; KPI trends.

7. Supply-Chain Security

Level	Characteristics	Indicative Evidence
0	No vendor inventory; contracts lack security terms.	—
1	Basic vendor list; informal due diligence.	Questionnaires by email.
2	Tiering; DPA templates; approval workflow.	Tiering model; DPA; approvals.
3	Assurance cadence by tier; onboarding controls; joint IR notification paths; SBOM requested when software delivered.	Evidence packs; onboarding checklist; IR clauses.
4	Fourth-party visibility for critical vendors; monitoring of advisories; VEX/provenance where available.	Sub-processor lists; VEX; attestation files.
5	Concentration risk tracked; tested exit plans/alternates; measurable vendor risk reduction over time.	Exit tests; concentration dashboards.

8. Incident Readiness

Level	Characteristics	Indicative Evidence
0	No plan; incidents handled ad-hoc.	—
1	Basic contact list; informal steps; no exercises.	Contact sheet.
2	IR policy/playbooks drafted; severity schema; initial exercises.	Policy; playbooks; tabletop notes.
3	Defined roles/RACI; triage/case mgmt; regulator/vendor/customer notification paths.	RACI; case samples; notification logs.
4	Forensics process; post-incident reviews (CAPA); integration with Monitoring & Detection and legal/comms.	Chain-of-custody; PIRs; CAPA logs.
5	Continuous improvement loop, scenario libraries, and measured MTTD/MTTR improvements.	Scenario sets; trend packs.

9. Business Continuity & Resilience

Level	Characteristics	Indicative Evidence
0	No BIA; no documented recovery plans.	—
1	Basic backup routine; untested plans.	Backup logs.
2	BIA with RTO/RPO; DR/continuity plans drafted; call trees.	BIA register; plans; call list.
3	Restoration tests; alternate site/workarounds; supplier continuity checks.	Test reports; workaround docs; supplier attestations.
4	Planned failovers; crisis comms templates; lessons learned drive plan updates.	Failover reports; templates; PIRs.
5	Validated resilience patterns (active/active etc.);	Resilience KPIs; exit drill

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Level	Characteristics	Indicative Evidence
	measurable downtime reduction; exit/transition drills for key suppliers.	records.

10. Privacy & Data Protection

Level	Characteristics	Indicative Evidence
0	No privacy policy; unmanaged processing; no rights handling.	—
1	Notices exist; consent tracking partial; ad-hoc grievance handling.	Notice text; emails.
2	Processing register; consent logs; DPR intake; retention schedule.	Registers; consent logs; retention policy.
3	DPIA/threshold reviews for higher-risk use cases; processor oversight; deletion/anonymization jobs.	DPIAs; DPA/agreements; job logs.
4	Preference portals; SLAs for DPR; breach response linkage with IR; privacy by default.	Portal screenshots; SLA reports; IR link.
5	Program metrics improve over time; proactive minimization; independent assurance where applicable.	Trend metrics; assurance reports.

11. Culture, Training & Awareness

Level	Characteristics	Indicative Evidence
0	No training; policies unknown to staff.	—
1	Annual awareness email; low completion.	Attendance list.
2	Role-based curriculum; onboarding/offboarding coverage; contractor inclusion.	Curricula; LMS setup; clauses.
3	Simulations (phishing/tabletops); remediation follow-ups; speak-up mechanisms.	Campaign reports; AARs; hotline logs.
4	Metrics used to tune content; leadership tone; near-miss reporting culture.	KPI pack; comms; near-miss logs.
5	Demonstrable behavior change and incident detection uplift tied to training.	Trend analysis; linkage to IR metrics.

12. Monitoring & Detection

Level	Characteristics	Indicative Evidence
0	No centralized logging; issues found by users.	—
1	Manual log pulls; few/no alerts.	Exports.
2	Partial centralization; basic alerts; informal triage.	Collector configs; alert list.
3	SIEM/EDR in place; documented use cases; structured triage/escalation; tickets link to alerts.	Dashboards; runbooks; cases.
4	Detection engineering lifecycle; intel enrichment; SOAR automation (safe actions); coverage and quality metrics.	Rule repo/tests; SOAR runs; KPI pack.
5	Continuous tuning with emulations; coverage tracked vs. top risks; backlog SLOs; improving MTTD/MTTR.	Emulation reports; coverage map; SLOs.

How to Use This Annex

1. For each domain, locate the description that most closely matches actual practice.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

2. Record the numeric level (0–5) in the self-assessment workbook.
3. Attach at least one piece of evidence corresponding to the level claimed.
4. Use the computed domain averages and radar visualization to plan improvement priorities.

DRAFT

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Annex B — Manufacturing Pilot Data-Collection Template

NIRMATA Framework v1.0

B.1 Purpose

This annex standardizes the information that participating organizations must provide during the manufacturing-sector pilot.
It ensures consistent, anonymized data capture across **MSME**, **mid-size**, and **large** enterprises so that aggregated national metrics are valid and comparable.

All collected data remain confidential and are used solely for statistical maturity analysis and anonymized benchmarking.

B.2 Submission Format

- **Preferred file type:** XLSX or CSV (UTF-8).
- **Alternative:** JSON payload for portal API.
- **Frequency:** Initial baseline and one follow-up after 90 days.
- **Record unit:** One record = one manufacturing site or plant.

Annex B — Section B.3 Data Elements (Clean Rendering)

Field Group	Field Name	Description	Format / Example	Mandatory
1 – Organization Profile	org_name	Legal name of the entity	Acme Auto Parts Pvt Ltd	✓
	site_id	Internal site or plant ID	PUNE-01	✓
	enterprise_type	MSME / Mid-Size / Large	MSME	✓
	sector_subtype	Manufacturing sub-sector	Automotive	✓
	employee_count	Headcount at site	280	✓
	annual_turnover_inr	Annual turnover (₹ crores)	12	
	contact_person	Assessment lead	Rajesh Kumar	✓
	designation	Role or title	Plant Head / CISO / DPO	✓
	email	Contact email ID	rajesh.kumar@acmeauto.in	✓
	region_state	State / UT	Maharashtra	✓
2 – Assessment Meta	assessment_date	Date of assessment	2025-06-10	✓
	assessment_type	Baseline /	Baseline	✓

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Field Group	Field Name	Description	Format / Example	Mandatory
		Follow-up / Verified		
	assessor_name	Name of verifier (blank for self-assessment)	—	
	ecf_rating	Evidence Confidence Factor average (0.5–1.0)	0.8	✓
3 – Domain Scores	dom01_governance … dom12_ai	Numeric 0–5 values for each domain	0 – 5	✓
	weighted_total	Auto-computed overall maturity score	3.4	✓
	target_next_cycle	Target maturity for next review	4.0	
4 – Evidence References	evidence_path	Folder path or portal upload ID	/evidence/PUNE-01/	✓
	evidence_items	Count of documents attached	45	✓
	evidence_verified_by	Internal reviewer name	QA Manager	
	peer_review_done	Peer review completed (Y/N)	Y	
5 – Operational Metrics	incidents_reported	No. of incidents in past 12 months	3	
	phishing_rate	% of users clicked test phish	18 %	
	mfa_coverage	% accounts with MFA enabled	92 %	
	vendor_count	Active vendors with data access	27	
	privacy_requests	Data-subject	2	

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Field Group	Field Name	Description	Format / Example	Mandatory
		requests received		
	ot_assets_count	OT devices monitored	148	
6 – Follow-Up Action Plan	top3_actions	Comma-separated improvement actions	MFA enforcement, OEM VPN policy, Phishing drill	✓
	action_owner	Responsible manager	IT Manager	✓
	target_date	Completion date	2025-09-30	✓
7 – Confidentiality Flags	publish_permission	Consent to publish anonymized data (Y/N)	Y	✓
	share_with_association	Permit sectoral benchmarking (Y/N)	Y	

B.4 Optional Attachments

1. **Governance Structure Chart** (PDF)
2. **Risk Register Snapshot** (XLSX / CSV)
3. **OT Network Diagram** (PNG / PDF)
4. **Incident Response Plan** (DOCX)
5. **Privacy Notice and Grievance Policy** (PDF)
6. **Training Attendance Summary** (CSV)
7. **Top Five Metrics Dashboard** (PNG / CSV)

B.5 Data-Quality Rules

Rule ID	Requirement	Validation Logic
DQ-01	All 12 domain scores must be numeric 0–5.	Reject otherwise.
DQ-02	`weighted_total` auto-recomputed server-side.	Portal calculation.
DQ-03	Evidence folder must contain ≥ 1 file per domain.	Warning if missing.
DQ-04	`assessment_type = Verified` requires assessor_name + ECF ≥ 0.9.	Enforced.
DQ-05	PII limited to contact fields; no employee records uploaded.	Privacy rule.

B.6 Anonymization and Use

- Organization names may be hashed (SHA-256) for aggregation.
- Only domain-level and overall scores appear in public benchmarks.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- All files stored within India in ISO 27001-certified facilities.
- Retention period = 12 months post-assessment, then securely purged.

B.7 Sample Record Excerpt (CSV)

```
org_name,site_id,enterprise_type,assessment_date,dom01_governance,...,dom12_ai,weighted_total,ecf_rating
Acme Auto Parts Pvt Ltd,PUNE-01,MSME,2025-06-10,3,3,3,2,3,2,3,2,2,3,2,1,2.7,0.8
```

B.8 Validation and Submission Process

1. **Local Validation:** Use the Excel macro to verify field completeness.
2. **Upload Portal:** Submit via https://elytrasecurity.com/trustin/portal.
3. **System Checks:** Automated validation per rules DQ-01–DQ-05.
4. **Acknowledgment:** Email receipt with submission ID.
5. **Peer Sampling:** 10 % records checked by sector mentor for quality.
6. **Final Lock:** Record status → "Accepted for Analysis".

B.9 Output to National Dashboard

Metric	Aggregation Method	Reporting Frequency
Average Maturity Score per Domain	Mean across validated records	Quarterly
Distribution of ECF Ratings	Histogram (High/Med/Low)	Quarterly
MSME vs Mid/Large Comparative Radar	Weighted averages	Half-yearly
Top Five Improvement Domains	Count of low-score areas ≤ 2 per submission	Annual

B.10 Responsibilities of Participants

- Provide truthful data and retain supporting evidence for 12 months.
- Participate in post-pilot feedback survey.
- Nominate a site representative for clarifications.
- Notify Elytra Security of any errors or withdrawal requests within 7 days.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Annex C — Assessor Guide

NIRMATA Framework v1.0

C.1 Purpose

This annex provides structured guidance for assessors, verifiers, and peer reviewers applying the **NIRMATA Framework**. It defines assessment methodology, evidence-confidence weighting, sampling procedures, and ethical requirements to ensure uniform scoring and defensible results.

C.2 Scope

Applies to:

- Internal self-assessors (Levels 0 – 3)
- Third-party verifiers and auditors (Levels 4 – 5)
- Peer reviewers participating in sector or association-led benchmarking

C.3 Assessor Qualifications

Category	Minimum Requirement	Preferred Credential
Lead Assessor	≥ 5 years in infosec or privacy governance	ISO 27001 LA / CISA / CISSP / DPDP-certified auditor
Technical Assessor (OT/AI)	≥ 3 years OT or AI risk experience	IEC 62443 practitioner / ISO 42001 lead implementer
Peer Reviewer	Independent of audited entity	Industry or academic expert recognized by Elytra Security
Ethics Declaration	Required annually by all assessors	Conflict-of-interest form (Appendix C-1)

C.4 Assessment Methodology

Preparation

- Obtain latest NIRMATA Workbook and Annex A ladders.
- Review prior assessment results if available.
- Define assessment scope (organization / site / process).

Evidence Collection

- Collect one primary and one supporting artifact per question minimum.
- Validate authenticity (timestamps / ownership / signatures).
- Tag each artifact with domain and level indicator.

Scoring

- Apply 0–5 response scale per Annex A.
- Record justification ≤ 30 words in Workbook notes.
- Apply **Evidence Confidence Factor (ECF)** per C.6.

Sampling

- Minimum sample = 25 % of evidence files per domain (≥ 5 items).

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- For multi-site enterprises ≥ 3 sites or 10 % of plants — whichever greater.
- Randomize sample selection using Portal tool or RNG.

Validation

- Verify dates (≤ 12 months old).
- Ensure cross-consistency between policy and practice evidence.
- Mark ECF = 0.5 if evidence cannot be verified.

Consolidation

- Compute Domain Score → Weighted Score → ECF-adjusted Total.
- Review outliers (> 1.5 variance between domains).
- Obtain management sign-off on results before submission.

C.5 Evidence Hierarchy

Evidence Type	Description	ECF Baseline
Primary Evidence	Signed policy, audit report, system log	1.0
Supporting Evidence	Screenshots, emails, training records	0.8
Indicative Evidence	Verbal confirmation, drafts	0.5
Contradictory	Inconsistent or out-of-date data	Reject

C.6 Evidence Confidence Factor (ECF)

Level	Definition	Multiplier
High	Fully documented and verified by system artifact or signed audit	1.0
Medium	Partially verified documentation / screen capture / internal memo	0.8
Low	Assertion without proof or dated evidence	0.5

Apply ECF to domain averages as:

Adjusted Score = Domain Score × ECF multiplier

C.7 Verification Levels and Reporting

Level	Verification Mechanism	Report Output	Validity
0 – 3	Internal self-assessment by organization	Internal scorecard & action plan	1 year
4	Third-party assessment (sampled evidence + interviews)	Verified Maturity Report (Annex C-2 template)	2 years
5	Independent peer review + on-site validation + benchmark analysis	NIRMATA Resilient Trust Certificate & public listing	3 years

C.8 Sampling Protocol for Large Enterprises

- **Population:** All sites ≥ 10.
- **Sample:** √N + 1 sites rounded up.
- **Stratification:** include at least one high-risk (OT) and one support function.
- **Follow-up:** Non-conformities must be closed within 60 days.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

C.9 Peer Review and Calibration

- 10 % of verified reports per quarter selected for peer calibration.
- Reviewers compare scoring rationale and evidence interpretation.
- Consensus variance > ± 0.5 triggers re-training of assessor pool.
- Summary statistics published annually for transparency.

C.10 Ethical Code of Conduct

1. **Independence:** Avoid financial or familial relationships with assessed entity.
2. **Confidentiality:** Handle all documents as restricted under NDAs.
3. **Objectivity:** Base scores solely on evidence presented.
4. **Non-Solicitation:** Assessors shall not sell consulting services to clients they audit within 12 months.
5. **Data Protection:** Store all assessment records within India and purge after validity expiry.

Violations may lead to suspension from the Verifier Registry.

C.11 Report Structure (Annex C-2 Template Summary)

1. Executive Summary (Organization, Scope, Assessor)
2. Maturity Radar and Domain Scores
3. Evidence Summary Table (High/Medium/Low)
4. Non-Conformity and Improvement Register
5. Verification Statement and Validity Period
6. Signatures (Assessor / Organization / Elytra Verifier Registry)

C.12 Appeals and Re-Verification

- Organizations may appeal a score within 30 days of report receipt.
- Appeals heard by Verification & Ethics Panel within 45 days.
- Outcomes: Confirm, Revise, or Re-audit within 90 days.
- Revised reports supersede previous records in the portal.

C.13 Continuous Improvement for Assessors

- Attend annual calibration workshops run by Elytra Security.
- Complete minimum 8 CPD hours on DPDP / AI governance topics.
- Maintain assessment log (entities, dates, domains scored).
- Peer feedback mandatory for renewal of Verifier status every 3 years.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

C.14 Submission and Archival

All verified reports must be submitted through the TRUST-IN Portal within **15 working days** of completion.
The portal automatically archives signed PDF copies and stores metadata (ECF averages, non-conformities, expiry date).
Raw evidence remains with the organization; only reference hashes are retained centrally.

DRAFT

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Annex D — MSME Self-Certification Guide

NIRMATA Framework v1.0

(For small and medium manufacturing enterprises)

D.1 Objective

To help Indian MSMEs conduct a **self-assessment under TRUST-IN Bharat** without requiring certified auditors or consultants.
This guide explains, step-by-step, how to identify relevant information, gather evidence, answer each question in the Workbook, and issue a valid self-certification for maturity Levels 0 – 3.

D.2 Who Can Use This Guide

Role	Typical Position	Responsibility in Assessment
Owner / Managing Partner	Factory owner, Director	Approves final self-assessment and action plan
Plant Head / Production Manager	Operations lead	Provides safety, maintenance, and continuity evidence
Accounts / HR Head	Compliance custodian	Gathers training, contracts, employee records
IT / Maintenance Staff	System administrator	Provides network, access, and backup evidence

No special qualification or audit license is required. Honesty, accuracy, and documented proof are the only prerequisites.

D.3 Self-Assessment in Five Simple Steps

Step 1 – Download and Prepare

1. Get the latest **TRUST-IN Bharat Self-Assessment Workbook** (Excel/PDF).
2. Create a folder named `NIRMATA_Evidence_<PlantName>`.
3. Inside, make 12 sub-folders — one for each domain (Governance, Risk, Compliance, …, AI).

Step 2 – Collect Evidence

For each question in the Workbook:

- Find one **document**, **record**, or **screenshot** that shows the practice actually exists.
- Acceptable examples: signed policies, training attendance, vendor PO with security clause, CCTV log, or backup folder screenshot.
- If nothing exists, mark **"No"** and note it as an improvement item.

Use the checklist below as a quick reference:

Domain	Typical Places to Look	Example Proof
Governance	Board minutes, organization chart	Appointment letter of CISO/DPO
Risk	Maintenance logs, daily production issue book	List of top 5 risks
Compliance	Labour files, ESI/PF filings	Register of statutory filings

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Data Lifecycle	Server folder structure, paper file register	File retention sheet
Access Mgmt	Attendance logs, login credentials sheet	User list with privileges
OT / IoT	PLC inventory, machine list	Labelled asset register
Vendor	Purchase orders, contracts	Clause mentioning data or NDA
Incident / Continuity	Fire-drill reports, UPS logs	Emergency plan
Privacy	Employee consent forms	HR onboarding checklist
Culture	Induction training slides	Sign-in sheet
Metrics	Daily KPI dashboard	Quality metrics
AI Governance	Machine learning tools, design software	Email showing review approval

Step 3 – Answer Honestly

Use the following self-rating logic (no math needed):

Response	Score	Meaning
Yes	5	Practice exists and is followed regularly
Partial	3	Exists but not consistent or missing proof
No	0	Not yet done

If unsure, choose **Partial** and make a note to improve next quarter.

Step 4 – Compute Scores

1. Let the Excel workbook auto-calculate totals.
2. Verify the radar chart — this is your maturity picture.
3. Identify domains scoring below 3 and mark them for action.

Step 5 – Create Your Self-Certification

1. Review all answers with management.
2. Fill the declaration form below (printable or portal).
3. Sign, date, and keep on record.

D.4 MSME Self-Certification Declaration (Sample)

TRUST-IN Bharat / NIRMATA Self-Assessment Declaration

We hereby declare that the information provided in this self-assessment represents our organization's actual practices as on **[date]**.

We understand that this declaration covers maturity Levels 0 – 3 under the NIRMATA Framework and may be reviewed or sampled by Elytra Security or its authorized partners.

Organization: _____
Plant / Site: _____
Authorized Signatory: _____
Designation: _____
Signature & Date: ____

Attach:

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

- Workbook file (`.xlsx`)
- Evidence folder (zipped)
- Optional photographs or screenshots (≤ 10 MB)

D.5 Practical Tips for MSMEs

Area	Simple Low-Cost Actions	Typical Free Tools
Policy drafting	Use government or Elytra sample templates	Word / Google Docs
Backups	Store on external HDD or cloud	OneDrive / Google Drive
Access control	Create unique logins, change monthly	Windows accounts
Awareness	10-minute safety talk every month	PowerPoint / poster
Vendor checks	Add "data-confidentiality clause" in PO	Excel tracker
Incident log	Notebook for system failures	Paper or Notion
Privacy	Ask employees to sign consent form	Word template
Monitoring	Note date/time of system checks	Manual logbook

D.6 Recommended Assessment Rhythm

Quarter	Key Activity
Q1	Baseline assessment and evidence creation
Q2	Implement top 3 actions
Q3	Mid-year self-check (update workbook)
Q4	Annual declaration and upload to portal

D.7 Upgrading to Verified Levels 4–5

When the enterprise:

- Has consistent documentation for at least 12 months,
- Uses automated monitoring or dashboards, and
- Seeks public recognition or tender participation,

it may invite a **Certified Verifier** (from Annex C registry) to perform a sample-based verification and issue a formal **NIRMATA Verified Report**.

D.8 Common MSME Mistakes to Avoid

1. Copying templates without tailoring them.
2. Signing policies never implemented.
3. Keeping evidence only in personal email or phone.
4. Ignoring OT/IoT networks ("machines are offline" assumption).
5. Forgetting privacy notices on job forms.
6. Not training contract labour or vendors.

Avoiding these ensures credibility and smoother progression to higher maturity.

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

D.9 Retention and Follow-Up

- Keep all self-certification records for **one year**.
- Update evidence folders before re-assessment.
- Share anonymized results with industry association (optional).
- Encourage neighbouring MSMEs to adopt TRUST-IN Bharat — peer learning accelerates maturity.

DRAFT

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Annex E — Cross-Framework Concordance Matrix

NIRMATA Framework v1.0

Purpose. This annex maps the twelve NIRMATA domains to relevant clauses and control sets in Indian law and international standards to support audits, gap analysis, and adoption without duplication of effort.

E.0 Legend and Notes

- **DPDP** = Digital Personal Data Protection Act, 2023 (sections indicative; apply rules/notifications as issued).
- **CERT-In 2022** = Directions under Section 70B(6) of the IT Act (Apr 28, 2022).
- **ISO 27001:2022** = Management clauses (Clause 4–10) and **Annex A** control IDs (A.5–A.8).
- **ISO 27701:2019** = PIMS requirements: **6–8** (common), **Annex A** (PII controller) & **Annex B** (PII processor) controls.
- **ISO 42001:2023** = Artificial Intelligence Management System (AIMS) requirements (Clauses 4–10; Annexes as applicable).
- **NIST CSF 2.0** = Functions (**ID, PR, DE, RS, RC**), Categories (e.g., **PR.AA** for Identity Management), and representative Subcategories.
- **Coverage tags**: **P**=Primary alignment, **S**=Supporting/adjacent alignment.
- This is **normative guidance** for concordance; it does **not** replace compliance obligations.

E.1 Governance & Leadership

Framework	Reference	Coverage
DPDP	s.10 (duties of significant data fiduciary), s.8(3) (reasonable security safeguards), s.9 (DPO for SDF)	**P**
CERT-In 2022	Dir. 3 (logs), Dir. 5 (time sync), governance to ensure compliance	**S**
ISO 27001	Clauses 4–7, 9 (context, leadership, planning, support, performance); A.5.1, A.5.2 (policies, roles)	**P**
ISO 27701	5–7 (governance of PIMS), A.5.1.1 (roles & responsibilities)	**P**
ISO 42001	Clauses 4–7 (context, leadership, risk), governance of AI responsibilities	**S**
NIST CSF 2.0	**ID.GV** (Governance), **GV.PO** (policies), **GV.RR** (risk mgmt roles)	**P**

E.2 Risk Management

Framework	Reference	Coverage
DPDP	s.8(3) (reasonable security safeguards), DPIA expectation for high-risk (policy intent)	**S**
CERT-In 2022	Dir. 1 (report specified incidents), governance must identify/report	**S**
ISO 27001	Clause 6 (risk assessment & treatment), A.5.9 (threat intelligence)	**P**

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Framework	Reference	Coverage
ISO 27701	6–8 (privacy risk assessment), Annex A/B (risk for PII)	**P**
ISO 42001	Risk-based AI controls across lifecycle (Clauses 6, 8)	**P**
NIST CSF 2.0	**ID.RA** (Risk Assessment), **ID.RM** (Risk Management Strategy)	**P**

E.3 Compliance Management

Framework	Reference	Coverage
DPDP	s.7–11 (lawful basis, notice, DSRs, grievances), s.8(5) (breach intimation)	**P**
CERT-In 2022	Dir. 1 (6-hour reporting), Dir. 3 (log retention), Dir. 5 (NTP time sync)	**P**
ISO 27001	Clause 9–10 (performance & improvement), A.5.36 (compliance with legal)	**P**
ISO 27701	Annex A/B mapping to legal obligations, controller/processor responsibilities	**P**
ISO 42001	Clause 9 (evaluation & compliance), legal/ethics obligations for AI	**S**
NIST CSF 2.0	**GV.OV** (oversight), **GV.PO-06** (legal & regulatory reqs integrated)	**S**

E.4 Data Lifecycle & Classification

Framework	Reference	Coverage
DPDP	s.8(7) (retention linked to purpose), s.7 (notice incl. retention), data minimization implied	**P**
CERT-In 2022	Dir. 3 (logs retention min. 180 days), evidence preservation	**S**
ISO 27001	A.5.12–A.5.14 (classification, labeling, handling), A.5.10 (data deletion)	**P**
ISO 27701	Annex A/B (PII lifecycle, retention/deletion, records of processing)	**P**
ISO 42001	Data for AI models: provenance, quality, retention (Clauses 8, 9)	**S**
NIST CSF 2.0	**ID.IM** (Information Mgmt), **PR.DS** (Data Security)	**P**

E.5 Identity & Access

Framework	Reference	Coverage
DPDP	s.8(3) (security safeguards), processor obligations	**S**
CERT-In 2022	Log, time sync, incident reporting (supports accountability for IAM events)	**S**
ISO 27001	A.5.15–A.5.23 (access control, user registration, MFA, privileged access)	**P**
ISO 27701	Annex A/B (access control to PII)	**S**
ISO 42001	Access to AI systems/models & training data controls	**S**
NIST CSF 2.0	**PR.AA** (Identity Mgmt, AuthN, AuthZ), **PR.AC** (Access Control)	**P**

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

E.6 Operational Technology & IoT Security

Framework	Reference	Coverage
DPDP	Security safeguards (s.8(3)) apply to personal-data handling OT systems	**S**
CERT-In 2022	Incident types include critical infrastructure; logging/reporting	**S**
ISO 27001	A.5.7 (segregation), A.5.15–A.5.23 (access), A.8.16 (monitoring)	**S**
ISO 27701	Not OT-specific; applies when PII in OT HMIs/logs	**S**
ISO 42001	AI in industrial control (quality/maintenance): risk, monitoring	**S**
NIST CSF 2.0	**ID.AM** (Asset Mgmt), **PR.PS** (Platform Security), **DE.CM** (Monitoring)	**P**
Adj. Guidance	NIST SP 800-82 r3 / IEC 62443 (good practice baselines)	**P (adj.)**

E.7 Vendor & Supply-Chain Governance

Framework	Reference	Coverage
DPDP	s.8(7) (processors; contractual obligations); s.10 (SDF obligations)	**P**
CERT-In 2022	Third-party incident reporting expectations via principal entity	**S**
ISO 27001	A.5.19–A.5.22 (supplier relationships, security in agreements, monitoring)	**P**
ISO 27701	Annex A/B (controller–processor contracts for PII)	**P**
ISO 42001	Third-party AI services, datasets, and model risks	**S**
NIST CSF 2.0	**GV.SC** (Supply-Chain Risk Mgmt), **ID.SC** (SCM)	**P**

E.8 Incident Readiness

Framework	Reference	Coverage
DPDP	s.8(5) (personal-data breach intimation to Board/Authority/Data Principals)	**P**
CERT-In 2022	**Dir. 1** (6-hour reporting), **Dir. 3** (logs), **Dir. 5** (time sync)	**P**
ISO 27001	A.5.24–A.5.33 (IR processes), A.5.29 (business continuity ICT)	**P**
ISO 27701	Annex A/B (personal-data incident handling)	**P**
ISO 42001	Incident mgmt for AI systems & model drift/failure	**S**
NIST CSF 2.0	**RS** (Respond), **RC** (Recover), including RS.AN/RS.MI/RC.CO	**P**

E.9 Privacy & Data Protection

Framework	Reference	Coverage
DPDP	s.4–11 (lawful processing, notice, consent, DSRs, grievance, purpose/retention), s.10 (SDF DPO)	**P**
CERT-In 2022	Reporting overlaps when incidents involve personal data	**S**

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

ISO 27001	A.5.34 (privacy & PII protection)	**S**
ISO 27701	**Core PIMS** requirements; Annex A/B controls for DSR, consent, records	**P**
ISO 42001	PII in AI training/inference; transparency/fairness	**S**
NIST CSF 2.0	**GV.PO-07** (privacy considerations integrated); **ID.IM-03** (records of data)	**S**

E.10 Culture & Workforce Awareness

Framework	Reference	Coverage
DPDP	s.8(3) (reasonable safeguards → training/awareness implied)	**S**
CERT-In 2022	Capabilities to detect/report incidents require trained staff	**S**
ISO 27001	A.6.3 (awareness, education), A.5.17 (user responsibilities)	**P**
ISO 27701	Annex A/B (privacy awareness)	**S**
ISO 42001	Competence & awareness for AI roles (Clauses 7.2–7.3)	**S**
NIST CSF 2.0	**GV.OC** (oversight of cybersecurity workforce), **PR.AT** (Awareness & Training)	**P**

E.11 Monitoring & Detection

Framework	Reference	Coverage
DPDP	s.8(3/5) (demonstrable safeguards, breach intimation → requires metrics)	**S**
CERT-In 2022	Dir. 3 (logs), Dir. 1 (reportable metrics)	**S**
ISO 27001	Clauses 9–10 (measurement, evaluation, improvement), A.8.16 (monitoring activities)	**P**
ISO 27701	9–10 PIMS performance evaluation & improvement	**S**
ISO 42001	Clause 9 (monitoring AI performance, drift)	**S**
NIST CSF 2.0	**DE.CM** (Monitoring), **GV.OV-06** (performance measures)	**P**

E.12 AI Governance & Ethical Use

Framework	Reference	Coverage
DPDP	Fair and lawful processing principles; DPO/SDF obligations (where personal data in AI)	**S**
CERT-In 2022	Incident reporting applies to AI-related breaches	**S**
ISO 27001	General ISMS scaffolding (risk, change, supplier) around AI systems	**S**
ISO 27701	PII in training/inference; records & rights handling	**S**
ISO 42001	**Primary** AIMS controls across lifecycle: data, model, deployment, transparency, risk	**P**
NIST CSF 2.0	**ID.IM** (data governance), **PR.PS** (platform security), **GV.RR** (risk), AI profiles as available	**S**

E.13 Quick Mapping Index (by NIRMATA Domain → Top Control Sets)

NIRMATA Domain	ISO 27001 Annex A (key)	ISO 27701 (Annex A/B)	ISO 42001 (Clauses)	NIST CSF 2.0 Categories

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

1 Governance	A.5.1–A.5.2	A.5.1	4–7	ID.GV, GV.PO
2 Risk	A.5.9, Clause 6	A/B Risk	6	ID.RA, ID.RM
3 Compliance	A.5.36, Cl. 9–10	A/B Legal	9	GV.PO-06
4 Data Lifecycle	A.5.12–A.5.14, A.5.10	A/B Lifecycle	8–9	ID.IM, PR.DS
5 Access & Identity	A.5.15–A.5.23	A/B Access	8	PR.AA, PR.AC
6 OT/IoT	A.5.7, A.8.16 (+ 800-82/62443)	—	8–9	ID.AM, PR.PS, DE.CM
7 Vendor/Supply	A.5.19–A.5.22	A/B Processor	8	ID.SC, GV.SC
8 Incident/Continuity	A.5.24–A.5.33	A/B Incident	8–9	RS, RC
9 Privacy Ops	A.5.34	**Core**	8–9	GV.PO-07
10 Culture	A.6.3, A.5.17	A/B Awareness	7	PR.AT, GV.OC
11 Metrics/Monitoring	Cl. 9–10, A.8.16	9–10	9	DE.CM, GV.OV
12 AI Governance	— (scaffold)	PII cases	**Core**	ID/PR/GV (profiles)

E.14 Using the Concordance in Practice

1. **Start with NIRMATA domain score** → identify gaps.
2. **Check the table above** to locate the **nearest formal control** set to implement.
3. **Select evidence** that simultaneously satisfies NIRMATA and your chosen standard (e.g., ISO 27001 A.5.15 for MFA, also lifting NIST PR.AA).
4. **For verified levels (4–5)**, ensure your implementation can be traced to a **specific clause/control** and that **evidence is sampled** per Annex C.
5. **For MSMEs**, prioritize controls that give **dual compliance** (e.g., a privacy notice aligns with DPDP and ISO 27701; a simple IR plan aligns with CERT-In and NIST RS/RC).

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com

Annex F Crosswalk: Whitepaper ↔ Annex G

Numbering note: Annex G's pillar numbering is editorial and may differ from the Whitepaper body. The names in this table are canonical; use this crosswalk as the authoritative mapping between documents.

Table F.1 — Pillar mapping

Whitepaper Pillar	Annex G Pillar
Governance & Leadership	Governance & Leadership
Risk & Compliance	Risk & Compliance
Application & Product Security	Application & Product Security
Asset & Data Management	Asset & Data Management
Identity & Access	Identity & Access
Infrastructure Security	Infrastructure Security
Supply-Chain Security	Supply-Chain Security
Incident Readiness	Incident Readiness
Business Continuity & Resilience	Business Continuity & Resilience
Privacy & Data Protection	Privacy & Data Protection
Culture, Training & Awareness	Culture, Training & Awareness
Monitoring & Detection	Monitoring & Detection

DRAFT

© 2025 Elytra Security. TRUST-IN Bharat / NIRMATA Framework is licensed under CC BY-SA 4.0.
This framework is an open maturity and readiness assessment model to enable organizations to align with ISO 27001 / 27701 / 42001, NIST CSF 2.0, and India's DPDP Act 2023 requirements. It is not a certification scheme and does not replace any standard or audit framework.
Feedback and peer review: https://github.com/trustin-bharat/nirmata-site/issues. Email: trustin@elytrasecurity.com