# INDIAN CYBERSECURITY GUIDELINES
## & REGULATORY CIRCULARS

*Security Controls Mapping Matrix | Recommended Security Services | Tools Implementation Coverage*

| | |
|---|---|
| **Edition** | Version 1.0 — March 2025 |
| **Frameworks Covered** | CERT-In, DPDP, RBI, SEBI, IRDAI, NHB, DoT, NCIIPC, MeitY, IT Act |
| **Scope** | Government, BFSI, Telecom, Healthcare, Critical Infrastructure |
| **Prepared by** | IT Governance & Compliance Practice |

# SECTION 1 — INDIAN CYBERSECURITY GUIDELINES & REGULATORY CIRCULARS

## 1.1 National-Level Frameworks

### A. CERT-In Directives (MeitY)

The Indian Computer Emergency Response Team (CERT-In) operates under Section 70B of the IT Act, 2000 and issues binding cybersecurity directions to all entities operating in India.

| Guideline/Circular | Reference | Key Mandate |
|---|---|---|
| **CERT-In Directions 2022** | No. 20(3)/2022-CERT-In dated 28-Apr-22 | 6-hr incident reporting, 5-yr log retention, NTP synchronisation, KYC/UIDAI linkage, VPN/cloud logs |
| **CERT-In Amendment 2022** | Clarification issued 17-Jun-22 | Clarifications on VPN, virtual asset service providers, mandatory registration |
| **CERT-In Empanelment Scheme** | Guidelines for IS Audit Firms | Criteria for IS auditor empanelment, audit methodology, competency |
| **IT Act Sec 70A — NCIIPC** | NCIIPC Framework 2013/updated | Protection of Critical Information Infrastructure (Power, Finance, Telecom, Transport) |
| **CERT-In CISO Guidelines** | Advisory 2023 | CISO responsibilities, board-level reporting, IR planning |
| **CERT-In Ransomware Advisory** | Advisory May-2022 | Backup strategy, segmentation, patch mgmt, response playbook |

### B. IT Act 2000 & Amendments

| Section | Year | Relevance |
|---|---|---|
| **Section 43 & 43A** | 2000/2008 | Penalty for unauthorised access & breach of sensitive personal data |
| **Section 66 – 66F** | 2008 | Cybercrimes: hacking, identity theft, cyber terrorism, offensive content |
| **Section 69 – 69B** | 2008 | Interception, monitoring, decryption powers; blocking of unlawful content |
| **Section 70** | 2008 | Protected systems notification by Central/State Govt |
| **Section 70A/70B** | 2008 | NCIIPC & CERT-In establishment mandates |
| **SPDI Rules 2011** | 2011 | Sensitive Personal Data: collection, processing, disclosure, security practices |
| **IT (Intermediary) Rules 2021** | 2021 | Due diligence, grievance officer, content takedown, traceability |

### C. Digital Personal Data Protection Act 2023 (DPDP Act)

| Section | Requirement |
|---|---|
| **Sec 4–9** | Lawful processing, consent framework, deemed consent, notice requirements |

| | |
|---|---|
| **Sec 10** | Obligations of Significant Data Fiduciaries (SDF): DPIA, DPO appointment, audit |
| **Sec 11–12** | Rights of Data Principals: access, correction, erasure, nomination, grievance |
| **Sec 17** | Data localisation: personal data of children, certain cross-border restriction |
| **Sec 25** | Security safeguards: technical & organisational measures, breach notification to DPBI within 72 hrs |
| **Sec 33–40** | Data Protection Board of India (DPBI): adjudication, penalties up to ₹250 Cr |
| **DPDP Rules (Draft 2025)** | Consent manager regulations, DPIA format, cross-border whitelist, SDF criteria |

Note: DPDP Act 2023 supersedes IT (SPDI) Rules 2011 upon notification of relevant sections.

## 1.2 Sector-Specific Regulatory Guidelines

### A. Reserve Bank of India (RBI) — BFSI Sector

| Circular / Framework | Issued By / Year | Key Controls Required |
|---|---|---|
| **IT Framework for Banks** | RBI / 2016 | Risk governance, IS audit, BCP/DR, patch management, access control |
| **Cyber Security Framework for Banks** | RBI / Jun-2016 | Baseline cybersecurity controls, CISO, SOC, incident response, VAPT |
| **Master Direction – RBI IT** | RBI / Apr-2024 (updated) | Consolidated IT governance, audit, risk, IS policy for regulated entities |
| **Guidelines on Digital Lending** | RBI / 2022 | Data security, customer consent, LSP oversight, storage restrictions |
| **NBFC IT Guidelines** | RBI / 2023 | IT governance, IS audit, BCP, cybersecurity for NBFC-M, NBFC-D |
| **UPI / Payment System Guidelines** | NPCI / RBI | PCI-DSS alignment, tokenisation, fraud monitoring, AML controls |
| **Cloud Adoption Framework** | RBI / 2023 | Risk assessment, data residency, audit rights, exit clause for cloud |
| **Third-Party Risk Management** | RBI / 2023 | Vendor due diligence, contractual obligations, monitoring, exit strategy |
| **Customer Protection – Fraud** | RBI / 2017 | Zero liability, limited liability, dispute resolution for digital fraud |

### B. Securities & Exchange Board of India (SEBI)

| Circular | Reference / Year | Mandate |
|---|---|---|
| **Cyber Security & Resilience Framework** | SEBI / Jan-2019 | Governance, audit, SOC, incident response for Stock Exchanges, Depositories, Clearing |
| **SEBI CSCRF 2023 (Updated)** | SEBI / Aug-2023 | Extended to brokers, RTAs, AMCs; 4-hour reporting, recovery time objectives |
| **Cloud Adoption Guidelines** | SEBI / 2023 | Data localisation, risk assessment, exit management for market infrastructure |

| | | |
|---|---|---|
| **Cyber Audit – Qualified Auditors** | SEBI Circular 2020 | IS audit by CERT-In empanelled auditors, half-yearly audit cycle |
| **Algorithmic Trading Guidelines** | SEBI / 2012 & updates | System audit, kill switch, order-to-trade ratio, co-location security |
| **Social Engineering Advisory** | SEBI / 2022 | Employee training, phishing simulation, callback verification |

## C. IRDAI — Insurance Sector

| Circular | Reference | Key Requirement |
|---|---|---|
| **IRDAI Cybersecurity Guidelines 2023** | IRDAI / Jun-2023 | CISO, IS audit, cyber insurance, SOC, incident reporting within 6 hrs |
| **IRDAI Cloud Guidelines 2023** | IRDAI / 2023 | Risk assessment, data residency in India, vendor oversight |
| **IRDAI Data Localisation** | IRDAI Circular 2019 | Policyholder data must be stored within India |
| **IRDAI Information/Cyber Security Policy** | IRDAI / 2017 | Policy framework, VAPT, patch management, BCP/DR |

## D. DoT / TRAI — Telecom Sector

| Guideline | Year | Mandate |
|---|---|---|
| **Telecom Cybersecurity Rules 2024** | DoT / Nov-2024 | Incident reporting within 6 hrs, log retention 2 yrs, mandatory security audit |
| **TRAI Recommendations on Cybersecurity** | TRAI / 2023 | Security gateway, caller ID authentication, spam/fraud control |
| **Telecom Equipment Approval** | DoT TEC | Security testing of telecom equipment before deployment |
| **NCCS (National Cyber Coordination Centre)** | MHA / MeitY | Real-time threat intelligence, co-ordination between agencies |

## E. Healthcare — MoH, NHA, ABDM

| Guideline | Reference | Requirement |
|---|---|---|
| **Digital Health Security Guidelines** | MoH / 2023 | Health data classification, consent, encryption, interoperability security |
| **ABDM Security & Privacy Spec** | NHA / 2021 | PHR, ABHA number security, API gateway controls, consent artefact |
| **EHR Standards 2013 (revised)** | MoH | Audit trail, access control, data backup for electronic health records |

## F. Government / e-Governance — MeitY, NIC, GIGW

| Guideline | Authority | Applicability |
|---|---|---|
| **National Cybersecurity Policy 2013** | MeitY | Framework for protecting cyberspace; roles of agencies, capacity building |

| | | |
|---|---|---|
| **National Cybersecurity Strategy 2020** | PMO / NSA | Cyber sovereignty, resilience, awareness, deterrence (7 pillars) |
| **GIGW – Govt IT Guidelines** | NIC / MeitY | Website security, WAF, SSL, accessibility, audit for Govt portals |
| **Rapid Assessment System (RAS)** | MeitY / 2022 | Continuous monitoring of Govt IT assets, vulnerability assessment |
| **STQC Audit Framework** | MeitY / STQC | IS audit, VAPT, WSTG testing for Govt IT projects |
| **Cloud Policy MeitY** | MeitY Empanelment | Use of MeitY-empanelled CSPs only for Govt cloud workloads |
| **NPKI Policy** | CCA / MeitY | National PKI, digital signatures, DSC usage, certificate management |

# SECTION 2 — SECURITY CONTROLS MAPPING MATRIX

The matrix below maps each security control domain against major Indian regulatory frameworks. Organisations should treat this as a minimum baseline — overlapping mandates require the stricter control to be implemented.

| LEGEND | ■ MANDATORY | ● RECOMMENDED | ○ ADVISORY / N/A |
|---|---|---|---|

| Control Domain | CERT-In | DPDP | RBI | SEBI | IRDAI | DoT | Govt / MeitY |
|---|---|---|---|---|---|---|---|
| Governance & Policy | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| Risk Assessment | Advisory | Mandatory (SDF) | Mandatory | Mandatory | Mandatory | Mandatory | Recommended |
| Asset Management | Mandatory | Recommended | Mandatory | Mandatory | Mandatory | Mandatory | Recommended |
| Access Control / IAM | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| Privileged Access Mgmt | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| Data Classification | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Advisory | Mandatory |
| Encryption (Data at Rest) | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| Encryption (In Transit) | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| Network Security / FW | Mandatory | Recommended | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| Vulnerability Assessment | Mandatory | Advisory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| Penetration Testing | Mandatory | Advisory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| Patch Management | Mandatory | Recommended | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| Log Management / SIEM | Mandatory (5yr) | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory (2yr) | Mandatory |
| Security Monitoring / SOC | Mandatory | Advisory | Mandatory | Mandatory | Mandatory | Advisory | Recommended |
| Incident Response | Mandatory (6hr) | Mandatory (72hr) | Mandatory | Mandatory (4hr) | Mandatory (6hr) | Mandatory (6hr) | Mandatory |
| Data Loss Prevention | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Advisory | Recommended |
| Email Security | Recommended | Recommended | Mandatory | Recommended | Recommended | Recommended | Mandatory |
| Endpoint Protection | Mandatory | Recommended | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| BCP / Disaster Recovery | Recommended | Recommended | Mandatory | Mandatory | Mandatory | Mandatory | Recommended |
| Third-Party / Supply Chain | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory | Mandatory |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Cloud Security** | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** | Advisory | **Mandatory** |
| **Data Localisation** | N/A | Mandatory (children) | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** |
| **Security Awareness Training** | **Mandatory** | Recommended | **Mandatory** | **Mandatory** | **Mandatory** | Recommended | Recommended |
| **Consent & Privacy Mgmt** | N/A | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** | Recommended | **Mandatory** |
| **Audit & Compliance Review** | Mandatory (6mo) | Mandatory (annual) | **Mandatory** | Mandatory (6mo) | **Mandatory** | Mandatory (annual) | **Mandatory** |
| **DPIA / Privacy Impact Assess** | N/A | Mandatory (SDF) | Recommended | Recommended | Recommended | N/A | Recommended |
| **NTP Synchronisation** | **Mandatory** | N/A | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** |
| **Mobile Device Security** | Recommended | Recommended | **Mandatory** | Recommended | Recommended | Advisory | Recommended |
| **API Security** | Recommended | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** |
| **CISO Appointment** | Advisory | Mandatory (SDF) | **Mandatory** | **Mandatory** | **Mandatory** | Advisory | Recommended |

Notes: (1) 'SDF' = Significant Data Fiduciary as defined under DPDP Act. (2) Incident reporting timelines vary per regulator — organisations operating across sectors must meet the shortest applicable SLA (typically 4–6 hours). (3) This matrix is indicative; always refer to the primary circular text for authoritative requirements.

# SECTION 3 — RECOMMENDED SECURITY SERVICES & TOOLS IMPLEMENTATION

The following catalogue maps each security service to the recommended tooling, products available/used in India, and the regulatory frameworks they satisfy. Organisations should prioritise tools from CERT-In empanelled, MeitY-empanelled, and BIS-tested vendors where applicable.

## 3.1 Identity & Access Management (IAM)

| Security Service / Control | Implementation Tools | Indian/Global Products | Regulatory Alignment |
|---|---|---|---|
| **Multi-Factor Authentication** | TOTP, FIDO2/WebAuthn, Smart Card | Microsoft Entra ID, Okta, Cymmetri (India), authbridge | CERT-In, RBI, SEBI, DPDP |
| **Single Sign-On (SSO)** | SAML 2.0, OIDC, OAuth 2.0 | Okta, Azure AD, ForgeRock, Ping Identity | RBI IT Framework, SEBI CSCRF |
| **Privileged Access Management** | PAM Vault, Session Recording, JIT | Sectona (India), CyberArk, BeyondTrust, Delinea | CERT-In, RBI, SEBI |
| **Directory Services** | LDAP, AD, Cloud Directory | Active Directory, Azure AD DS, AWS IAM | CERT-In, RBI, Govt GIGW |
| **Identity Governance (IGA)** | Role mining, access certification | SailPoint, Saviynt, IBM ISIM | RBI, SEBI, IRDAI |

## 3.2 Network Security

| Security Service / Control | Implementation Tools | Indian/Global Products | Regulatory Alignment |
|---|---|---|---|
| **Next-Gen Firewall (NGFW)** | Stateful inspection, App-ID, IPS | Palo Alto, Fortinet, Check Point, Sophos, Cisco | CERT-In, RBI, SEBI, DoT |
| **Web Application Firewall (WAF)** | OWASP Top 10, rate limiting, bot mgmt | AWS WAF, Imperva, F5, Indusface (India), Cloudflare | CERT-In, RBI, SEBI, GIGW |
| **DDoS Protection** | Volumetric & application layer mitigation | Cloudflare, Akamai, AWS Shield, Radware, Tata Cliq | CERT-In, DoT Telecom Rules |
| **Intrusion Detection / Prevention** | Signature + anomaly detection | Snort/Suricata, Cisco Firepower, Vectra AI | CERT-In, RBI, SEBI |
| **Network Access Control (NAC)** | 802.1X, endpoint posture assessment | Cisco ISE, Aruba ClearPass, Forescout | RBI, SEBI |
| **Zero Trust Network Access** | Micro-segmentation, ZTNA proxy | Zscaler ZPA, Cloudflare Access, Palo Alto Prisma | RBI IT 2024, SEBI Cloud |
| **SD-WAN Security** | Encrypted overlay, SASE integration | Cisco Meraki, Fortinet SD-WAN, VMware VeloCloud | RBI, IRDAI, DoT |

## 3.3 Endpoint & Device Security

| Security Service / Control | Implementation Tools | Indian/Global Products | Regulatory Alignment |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Endpoint Detection & Response (EDR)** | Behavioural analysis, threat hunting | CrowdStrike, SentinelOne, Microsoft Defender, Quick Heal (India) | CERT-In, RBI, SEBI, IRDAI |
| **Mobile Device Management (MDM)** | Policy enforcement, remote wipe, containerisation | Microsoft Intune, VMware Workspace ONE, Jamf | RBI, IRDAI, Govt |
| **Data Loss Prevention (DLP)** | Content inspection, policy enforcement | GTB Technologies (used in India), Symantec DLP, Forcepoint, Microsoft Purview | CERT-In, DPDP, RBI, SEBI |
| **Application Whitelisting** | Execution control, allowlist policy | Carbon Black App Control, CrowdStrike App Control | CERT-In, RBI |
| **Patch Management** | Automated scanning, deployment, reporting | Microsoft WSUS/SCCM, Qualys PM, Ivanti, ManageEngine | CERT-In, RBI, SEBI |

## 3.4 Vulnerability Management & VAPT

| Security Service / Control | Implementation Tools | Indian/Global Products | Regulatory Alignment |
|---|---|---|---|
| **Vulnerability Scanner** | Network, web, cloud scanning | Rapid7 InsightVM (used in India), Tenable Nessus, Qualys, OpenVAS | CERT-In, RBI, SEBI, STQC |
| **Penetration Testing Platform** | Manual + automated exploitation | Metasploit, Cobalt Strike, Burp Suite, OWASP ZAP | CERT-In, RBI, SEBI, IRDAI |
| **Web Application Scanning** | DAST, SAST, IAST | Veracode, Checkmarx, OWASP ZAP, Rapid7 AppSpider | CERT-In, RBI, SEBI, STQC |
| **Red Team / TLPT** | Threat-led penetration testing | CERT-In empanelled auditors, TIBER-IN equivalent | RBI, SEBI, IRDAI |
| **Attack Surface Management** | External asset discovery, exposure mgmt | CyCognito, Mandiant ASM, Detectify | CERT-In Advisory, RBI |

## 3.5 Security Information & Event Management (SIEM) / SOC

| Security Service / Control | Implementation Tools | Indian/Global Products | Regulatory Alignment |
|---|---|---|---|
| **SIEM Platform** | Log aggregation, correlation, alerting | Microsoft Sentinel, Splunk, IBM QRadar, Securonix, LogRhythm | CERT-In (5-yr retention), RBI, SEBI |
| **Log Management / SOAR** | Playbook automation, orchestration | Splunk SOAR, Palo Alto XSOAR, IBM Resilient, Swimlane | CERT-In, RBI, SEBI CSCRF |
| **Threat Intelligence Platform** | IOC feeds, threat actor tracking | Mandiant TI, Recorded Future, MISP, ThreatConnect, CERT-In feeds | CERT-In, NCIIPC, RBI |
| **Managed SOC / MSSP** | 24×7 monitoring, L1/L2/L3 analysts | Tata Communications TSOC, Wipro GSOC, HCL, IBM MSS | RBI, SEBI, IRDAI, CERT-In |
| **User Behaviour Analytics (UEBA)** | Insider threat, anomaly detection | Securonix UEBA, Exabeam, Microsoft Sentinel UEBA | RBI, DPDP, SEBI |

| | | | |
|---|---|---|---|
| **NTP / Time Synchronisation** | Stratum-1/2 NTP server configuration | chrony, ntpd, Windows NTP, Meinberg NTP appliances | CERT-In (mandatory) |

## 3.6 Data Security & Privacy

| Security Service / Control | Implementation Tools | Indian/Global Products | Regulatory Alignment |
|---|---|---|---|
| **Data Classification Engine** | Auto-tagging, sensitive data discovery | Microsoft Purview, BigID, Varonis, Spirion | DPDP, RBI, SEBI, CERT-In |
| **Encryption – Data at Rest** | AES-256, volume/column encryption | HashiCorp Vault, AWS KMS, Azure Key Vault, Thales HSM | CERT-In, DPDP, RBI, SEBI |
| **Encryption – Data in Transit** | TLS 1.2+, mTLS, VPN | Let's Encrypt, Sectigo, DigiCert, OpenSSL, Cisco AnyConnect | CERT-In, RBI, DoT |
| **Database Activity Monitoring** | Query-level audit, anomaly, masking | Imperva DAM, IBM Guardium, McAfee DAM | RBI, DPDP, SEBI |
| **Privacy Management / Consent** | Consent lifecycle, DPIA, DSR workflow | OneTrust, TrustArc, MineOS, Securiti.ai | DPDP Act 2023, RBI, IRDAI |
| **Data Masking / Tokenisation** | Static/dynamic masking, PAN tokenisation | Informatica IDQ, IBM InfoSphere, Thales, Protegrity | DPDP, RBI (payment data), PCI-DSS |
| **Digital Rights Management** | Content protection, information barriers | Microsoft Purview AIP, Vera, Sealpath | DPDP, RBI, SEBI |

## 3.7 Cloud & Application Security

| Security Service / Control | Implementation Tools | Indian/Global Products | Regulatory Alignment |
|---|---|---|---|
| **Cloud Security Posture Mgmt (CSPM)** | Misconfiguration detection, compliance | Prisma Cloud, Wiz, Microsoft Defender for Cloud, Lacework | RBI Cloud 2023, SEBI, CERT-In |
| **Cloud Workload Protection (CWPP)** | Runtime protection, container security | Aqua Security, Sysdig, Twistlock, CrowdStrike Falcon Cloud | RBI, SEBI, CERT-In |
| **Container & K8s Security** | Image scanning, network policy, RBAC | Aqua, Trivy, OPA Gatekeeper, Falco, Snyk | RBI Cloud, CERT-In |
| **API Gateway & Security** | Auth, rate-limiting, input validation | AWS API Gateway, Apigee, Kong, MuleSoft, Tyk | DPDP, RBI, SEBI, DoT |
| **DevSecOps / Shift-Left** | SAST, DAST, SCA in CI/CD pipeline | Snyk, SonarQube, Checkmarx, GitHub Advanced Security | RBI, SEBI, CERT-In |
| **CASB – Cloud Access Security** | Shadow IT discovery, DLP, access control | Microsoft Defender for Cloud Apps, Netskope, Zscaler | RBI, SEBI, IRDAI |
| **MeitY-Empanelled Cloud** | Gov workloads on approved CSPs | NIC Cloud, AWS India, Azure India, GCP India, CtrlS | MeitY Cloud Policy, CERT-In |

## 3.8 Incident Response & Business Continuity

| Security Service / Control | Implementation Tools | Indian/Global Products | Regulatory Alignment |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **IR Platform / SOAR** | Playbook, ticketing, communication | Palo Alto XSOAR, Splunk SOAR, IBM Resilient, ServiceNow SecOps | CERT-In (6hr), RBI, SEBI (4hr), IRDAI |
| **Digital Forensics & IR** | Evidence collection, memory forensics | Magnet AXIOM, Cellebrite, FTK, Volatility, Autopsy | CERT-In, IT Act Sec 65B |
| **Backup & Recovery** | Air-gapped, immutable backups, RTO/RPO | Veeam, Commvault, Rubrik, Cohesity, Veritas | RBI, SEBI, IRDAI |
| **BCP / DR Orchestration** | Runbook automation, failover testing | Zerto, AWS DRS, Azure Site Recovery, VMware SRM | RBI, SEBI, IRDAI, CERT-In |
| **Crisis Communication** | Secure messaging, notification workflows | Everbridge, PagerDuty, Mattermost, Slack (govt-grade) | CERT-In, SEBI, RBI |

## 3.9 Governance, Risk & Compliance (GRC)

| Security Service / Control | Implementation Tools | Indian/Global Products | Regulatory Alignment |
|---|---|---|---|
| **GRC Platform** | Policy mgmt, risk register, controls library | ServiceNow GRC, MetricStream, RSA Archer, SAP GRC | All Regulators |
| **IS Audit Management** | CERT-In audit workflow, evidence mgmt | Diligent, Riskonnect, Auditboard, TeamMate+ | CERT-In, STQC, RBI, SEBI |
| **Compliance Monitoring** | Continuous control monitoring, dashboards | Tugboat Logic, Hyperproof, Vanta, Drata | RBI, SEBI, IRDAI, CERT-In |
| **Third-Party Risk Management** | Vendor assessment, scoring, contracts | BitSight, SecurityScorecard, ProcessUnity, OneTrust TPRM | RBI TPRM 2023, CERT-In, SEBI |
| **Policy & Awareness Platform** | Policy lifecycle, phishing simulation, LMS | KnowBe4, Proofpoint SAT, Mimecast, Cofense | CERT-In, RBI, SEBI, IRDAI |

# SECTION 4 — IMPLEMENTATION ROADMAP & COMPLIANCE TIMELINE

Organisations should implement security controls in a phased approach based on regulatory mandates and risk exposure. The roadmap below provides a recommended sequencing aligned with Indian regulatory timelines.

## 4.1 Phase-wise Implementation Plan

| Phase | Timeline | Priority Controls | Regulatory Driver |
|---|---|---|---|
| **Phase 1 – Foundation** | Month 1–3 | CISO appointment, IS Policy, Asset inventory, IAM/MFA, NTP sync, Incident Response Plan | CERT-In 2022, RBI, DPDP Sec 25 |
| **Phase 2 – Detection** | Month 3–6 | SIEM deployment, SOC setup, VAPT cycle 1, Patch management, Log retention (5yr) | CERT-In, RBI IT, SEBI CSCRF |
| **Phase 3 – Data Protection** | Month 6–9 | Data classification, DLP deployment, Encryption (rest & transit), Consent framework, DPIA | DPDP Act, RBI, SEBI |
| **Phase 4 – Advanced Defense** | Month 9–12 | PAM, Zero Trust, Cloud CSPM, UEBA, Red Team exercise, Supply Chain assessment | RBI Cloud 2023, SEBI, IRDAI |
| **Phase 5 – Continuous Compliance** | Ongoing | Quarterly VAPT, Annual audit, GRC automation, Awareness training, Threat intelligence | All Regulators |

## 4.2 Key Regulatory Deadlines & Reporting Obligations

| Obligation | Regulator | Timeline / Frequency | Format / Destination |
|---|---|---|---|
| **Cyber Incident Reporting** | CERT-In | Within 6 hours of detection | CERT-In portal / email |
| **Data Breach Notification** | DPBI (DPDP Act) | Within 72 hours | DPBI portal + Data Principal |
| **Cyber Incident Reporting** | RBI (Banks) | Within 6 hours (initial); RBI mandated report within 24 hrs | RBI DAKSH portal |
| **Cyber Incident Reporting** | SEBI (MII/Broker) | Within 4 hours; root cause within 21 days | SEBI SCORES / email |
| **Cyber Incident Reporting** | IRDAI | Within 6 hours | IRDAI designated email |
| **Cyber Incident Reporting** | DoT / Telecom | Within 6 hours | CERT-In + DoT portal |
| **IS Audit Report Submission** | SEBI (Stock Exchange) | Half-yearly | SEBI Reporting Portal |

| | | | |
|---|---|---|---|
| **IS Audit Report** | RBI | Annual (some half-yearly) | RBI / Board / Audit Committee |
| **VAPT Report** | CERT-In empanelled | Annual minimum; half-yearly for critical | Internal + Regulator on request |
| **Annual Compliance Report** | IRDAI | Annual | IRDAI / Board |
| **Log Retention** | CERT-In | 5 years minimum | On-premise / MeitY-approved cloud |
| **Log Retention** | DoT Telecom Rules 2024 | 2 years | TSP infrastructure |

## 4.3 CERT-In Empanelment & Audit Requirements

All organisations subject to CERT-In Directions must engage CERT-In empanelled IS auditors for mandatory security audits. Key requirements:

- IS audit must be conducted by empanelled firms listed on cert-in.org.in/empanelled-auditors
- Audit scope: network, application, cloud, physical security, governance review
- Audit cycle: minimum annual; critical sectors every 6 months
- Audit report must be submitted to CERT-In upon request within 6 hours during an incident
- STQC (Standardisation, Testing & Quality Certification) audits required for Govt IT projects under MeitY

## 4.4 Tool Selection Criteria for Indian Regulatory Compliance

| Criterion | Guidance |
|---|---|
| **MeitY Cloud Empanelment** | For Government organisations, prefer MeitY-empanelled cloud service providers (NIC, AWS India, Azure India, GCP India, CtrlS, E2E Networks) |
| **Data Residency** | Tools must support Indian data centres for log and sensitive data storage per RBI, SEBI, IRDAI, and DPDP requirements |
| **CERT-In Empanelment (Auditors)** | Security audit tools must be operated by or in conjunction with CERT-In empanelled auditors for audit validity |
| **BIS / STQC Certification** | Prefer products with BIS (IS 17789) or STQC testing certification for government deployments |
| **Local Support & SLA** | Critical security tools must have India-based support with documented SLA meeting incident reporting windows |
| **Encryption Standards** | Products must support AES-256 (at rest), TLS 1.2+ (in transit), and Indian PKI (DSC/NPKI compatibility) |
| **Audit Trail** | All security tools must generate tamper-evident, time-stamped logs exportable to SIEM/CERT-In format |
| **Integration Capability** | Tools must integrate with existing SIEM, GRC, and ITSM platforms via API/REST/SYSLOG |

## 4.5 Quick-Reference: India-Specific Security Vendors & Products

| Indian/India-Deployed Vendor | Product / Service | Regulatory Use Case |
|---|---|---|

| | | |
|---|---|---|
| **Cymmetri (India)** | Identity & Access Management, PAM | CERT-In, RBI, SEBI – IAM/PAM compliance |
| **Sectona Security (India)** | Privileged Access Management | CERT-In, RBI IT Framework – PAM |
| **GTB Technologies (India presence)** | Data Loss Prevention | CERT-In, DPDP, RBI – DLP enforcement |
| **Vehere (India)** | Network Traffic Analytics / NDR | CERT-In, RBI – SOC monitoring |
| **Indusface (India)** | WAF, DAST, Managed AppSec | CERT-In, RBI – Web application protection |
| **Quick Heal / Seqrite (India)** | Endpoint Security, UTM, MDM | CERT-In, RBI – Endpoint protection |
| **Tata Communications / TSOC** | Managed SOC, DDoS, SD-WAN | CERT-In, RBI, SEBI – MSSP/SOC services |
| **E2E Networks (India)** | MeitY-empanelled Cloud | MeitY, RBI Cloud – Govt workloads |
| **NIC Cloud (India)** | Government Cloud (GI Cloud) | MeitY mandatory – Central/State Govt apps |
| **CtrlS / Yotta (India)** | Tier-IV Datacenter, Cloud | RBI, SEBI, IRDAI – Data residency compliance |
| **Black Box India** | IT Security, CERT-In Audit, Network | CERT-In empanelled IS auditor services |
| **STQC Directorate** | Third-party IT testing, IS audit | MeitY, Govt IT project security audits |
| **C-DAC (India)** | Cryptography, PKI, NPKI, BOSS OS | Govt, NPKI infrastructure, sovereign tech |
| **Authbridge (India)** | Identity verification, BGV, KYC | DPDP, RBI KYC, PMLA compliance |
| **Kyndryl India** | Managed Security Services, SOC | RBI, SEBI – Large enterprise MSSP |

**DISCLAIMER:** *This document is a reference guide based on publicly available Indian regulatory frameworks as of March 2025. Regulatory requirements are subject to change. Always consult the primary circular/directive from the respective regulator and engage legal counsel for compliance decisions. CERT-In, RBI, SEBI, IRDAI, DoT, MeitY circulars are the authoritative sources.*