



India Cyber Compliance Roadmap 2026 to 2027

The CXO Timeline

India Cyber Compliance Roadmap 2026 to 2027: The CXO Timeline

The Digital Personal Data Protection (DPDP) Rules, notified on 13 November 2025, set India's cyber compliance timeline. The Consent Manager framework activates on 13 November 2026. Hard enforcement of the DPDP Act arrives on 13 May 2027 with penalties up to ₹250 crore. The Indian Computer Emergency Response Team (CERT-In) six-hour reporting clock runs in parallel. The Securities and Exchange Board of India (SEBI), the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India (IRDAI) and the Central Electricity Authority (CEA) each impose sectoral overlays. 2026 is the build year. 2027 is the penalty year.

Table of Contents

1. <u>What Does the Indian Cyber Regulatory Landscape Look Like?</u>	04
2. <u>What Are the Critical India Cyber Compliance Dates in 2026 to 2027?</u>	05
3. <u>The Anchor Regulation: DPDP Act and Rules</u>	06
4. <u>The Always-On Regulation: CERT-In</u>	07
5. <u>The Sectoral Overlays</u>	07
6. <u>The Convergence Challenge: One Estate, Many Clocks</u>	08
7. <u>The Technical Controls That Satisfy Multiple Regulators</u>	08
8. <u>What Indian Enterprises Should Do in 2026</u>	10
9. <u>FAQ</u>	11

What Does the Indian Cyber Regulatory Landscape Look Like?

Table 1: The Indian Cyber Regulatory Landscape

Regulation / Authority	Who It Applies To	What It Covers	Headline Date
DPDP Act 2023 and DPDP Rules 2025	Every Data Fiduciary processing personal data of individuals in India	Lawful processing, data principal rights, reasonable security safeguards, breach notification, Significant Data Fiduciary (SDF) duties	Hard enforcement 13 May 2027
CERT-In Direction (2022)	Body corporates, intermediaries, data centres, service providers, government	Mandatory reporting of specified cyber incidents within six hours	In force
National Critical Information Infrastructure Protection Centre (NCIIPC) (Section 70A, IT Act 2000)	Designated critical information infrastructure	Conformity Assessment Framework integrating IEC 62443 / IS 16335, ISO 27000, NIST and CIS	In force
RBI cybersecurity directions for banks and regulated financial entities	Banks, NBFCs, payment system operators	IT framework, periodic Vulnerability Assessment and Penetration Testing (VAPT), rapid incident reporting, data localisation for payment data	In force
SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) (Aug 2024 master circular plus subsequent advisories)	22 categories of SEBI-regulated entities: Market Infrastructure Institutions (MIIs), brokers, AMCs, depositories, custodians	ISO 27001 for MIIs and Qualified REs, regular VAPT, Cyber Capability Index (CCI), Software Bill of Materials (SBOM) for critical applications	In force; SBOM advisory 5 May 2026

Regulation / Authority	Who It Applies To	What It Covers	Headline Date
IRDAI Information and Cybersecurity Guidelines	Insurers and intermediaries	Annual VAPT, board-level CISO accountability, third-party risk, incident reporting	In force
CEA Cyber Security in Power Sector Guidelines 2021	Power-sector entities	Electronic security perimeters per IEC 62443 / IS 16335	In force
Department of Telecommunications (DoT) licensing: Unified Licence (UL) and UL Virtual Network Operator (UL-VNO)	Telecom and cloud-calling carriers	Lawful interception, data residency, security clauses in licence	In force

What Are the Critical India Cyber Compliance Dates in 2026 to 2027?

Table 2: Critical Dates 2026 to 2027

Date	Event
Throughout 2026	DPDP soft enforcement: guidance and warnings, no hard penalties yet
5 May 2026	SEBI AI Vulnerability Detection Advisory; SBOM mandate for critical applications at SEBI-regulated entities, among the first explicit sectoral SBOM mandates in Indian regulation
13 November 2026	DPDP Consent Manager framework activates. Consent Manager registration opens; only India-incorporated entities with ₹2 crore minimum net worth qualify to register as Consent Managers

Date	Event
Q1 2027	Industry-recommended SDF readiness window: appointed Data Protection Officer (DPO), appointed independent data auditor, completed Data Protection Impact Assessment (DPIA) for high-risk processing, ahead of the legal trigger
13 May 2027	DPDP hard enforcement. SDF obligations legally enforceable from this date. Data Protection Board can impose penalties up to ₹250 crore (US\$26.24 million) for major violations

The Anchor Regulation: DPDP Act and Rules

The DPDP Act is the single piece of regulation that touches every Indian enterprise. Rule 6 sets the technical control set: encryption at rest and in transit, access limited to authorised persons, audit logs retained for at least one year, the ability to detect and reconstruct an incident, and a breach reporting workflow to the Data Protection Board (without delay, with a detailed 72-hour follow-up). The wider control set sits in our DPDP Act Compliance Checklist.

Two pieces of DPDP need separate programmes of work.

Consent Manager framework

Activates 13 November 2026. Indian enterprises must rebuild consent capture so each purpose is recorded separately, retain consent artefacts as an audit trail, and build the API surface that lets a registered Consent Manager pull and update a principal's consent state. The deeper view sits in our Consent Manager Framework spoke.

Significant Data Fiduciary Obligations

For entities likely to be designated (large fintech, telecom, e-commerce, healthcare, social, mobility), additional duties of DPO appointment, annual independent audit and annual DPIA become legally enforceable on 13 May 2027. Industry consensus is that readiness should be in place by Q1 2027 to leave a buffer.

The Always-On Regulation: CERT-In

CERT-In's 2022 Direction requires reporting of specified cyber incidents within six hours of becoming aware. Categories include unauthorised access, identity theft, phishing attacks, data breaches and ransomware. The clock runs in parallel with DPDP's "without delay plus 72-hour" clock; the same incident can require two notifications to two regulators on two different timelines. The operational playbook for closing the six-hour window sits in our CERT-In 6-Hour Reporting Operational Playbook.

The Sectoral Overlays

DPDP and CERT-In are horizontal. Sectoral regulators layer on top.

RBI

The Reserve Bank of India's cybersecurity directions for banks and regulated financial entities cover the 2016 Cyber Security Framework for Banks, master directions on IT framework and outsourcing, and the April 2018 circular on data localisation for payment system data. Periodic VAPT for critical systems is mandatory; incident-reporting timelines are rapid and vary by directive.

SEBI

The SEBI CSCRF (August 2024 master circular plus subsequent technical clarifications) applies to 22 categories of regulated entities. ISO 27001 is mandatory for MIIIs and Qualified REs. Regular VAPT, the CCI for resilience scoring, and a dedicated SEBI incident-reporting portal are baseline. The 5 May 2026 advisory added an SBOM mandate for critical applications.

IRDAI

Insurers and intermediaries must run annual VAPT, name a board-accountable CISO and manage third-party cyber risk. IRDAI guidelines govern insurers themselves, not the policyholder requirements that underwriters flow through to corporate insureds (covered in our Cyber Insurance Controls piece).

CEA

The Cyber Security in Power Sector Guidelines 2021 require electronic security perimeters per IEC 62443 / IS 16335 for power-sector entities. See our IEC 62443 OT Security Roadmap.

DoT

UL and UL-VNO licensing impose lawful-intercept and data-residency clauses on telecom and cloud-calling carriers and their on-network customers. Relevant to enterprises deploying Webex Calling in India.

The Convergence Challenge: One Estate, Many Clocks

The hard truth most CISOs land in 2026 is that a single Indian estate is now answerable to four to six regulators at once. A BFSI enterprise running cloud calling for a contact centre must satisfy RBI cybersecurity norms, DPDP, CERT-In reporting, DoT licensing for the carrier handoff, and potentially SEBI CSCRF if it has capital-market exposure. A manufacturer with a regulated pharma unit overlays NCIIPC, CEA-equivalent obligations, customer audits to IEC 62443 and DPDP for HR data.

Sectoral regulators each impose their own rapid incident-reporting clocks, ranging from immediate to six hours, depending on the directive; CERT-In's six-hour rule applies in parallel to all. The instinct to run six compliance programmes in parallel is wrong. The right move is to map controls once and accept the overlap as a feature.

The Technical Controls That Satisfy Multiple Regulators

Most of DPDP Rule 6, the CERT-In incident detection workflow, the RBI IT framework, SEBI CSCRF and IRDAI annual cycle land on the same control set.

Table 3: Controls That Satisfy Multiple Regulators

Control	DPDP Rule 6	CERT-In	RBI	SEBI CSCRF	IRDAI
Encryption at rest and in transit	Yes	Detection signal	Yes	Yes	Yes
Phishing-resistant MFA on privileged access	Implicit via access control	Strongly recommended	Yes	Yes	Yes
Network segmentation between personal-data systems and the general estate	Yes	Reduces blast radius	Yes	Yes	Yes
Security Information and Event Management (SIEM) with one-year minimum log retention	Yes	Required to reconstruct an incident inside six hours	Yes	Yes	Yes
Endpoint Detection and Response (EDR) on endpoints and servers	Implicit via detection	Required for category coverage	Yes	Yes	Yes
Regular VAPT	Implicit via security safeguards	Useful for detection coverage	Mandatory	Mandatory	Annual mandatory
Incident response playbook with multi-regulator notification	Implicit	Six-hour reporting	Rapid reporting per directive	Immediate via SEBI portal	Yes
Named DPO / grievance officer	Yes, published	Operational contact	Yes (CISO)	Yes	Yes (CISO)

What Indian Enterprises Should Do in 2026

Six moves, in order.

- **Personal data inventory:** Map every store of personal data, structured and unstructured. Without this, every other DPDP step is theoretical.
- **Consent capture redesign:** For the 13 November 2026 Consent Manager activation, each purpose recorded separately, plain-language notice, a verifiable timestamp, API surface for the registered Consent Manager.
- **DPO / grievance officer:** Named, published, reachable. Build the data principal rights workflow behind a single orchestration layer.
- **Technical control set:** Phishing-resistant MFA, segmentation, SIEM with one-year retention, EDR, and named-user network access. Cisco ISE is the typical India choice for the network layer.
- **Multi-regulator incident response:** Update the playbook to fan out a single internal trigger to CERT-In, the DPDP Data Protection Board, the relevant sectoral regulator and the foreign principal where one exists.
- **SDF readiness:** Decide and document whether your organisation is likely to be designated, and start the DPO appointment, independent auditor selection and DPIA process now. Q1 2027 readiness is closer than it feels.

How Proactive Data Systems Helps

Proactive Data Systems is a Preferred Partner under the Cisco 360 Partner Program across Networking, Security, Collaboration, Cloud & AI, and Services. We design and deploy the technical control set that satisfies Rule 6, the CERT-In detection and reporting workflow and the sectoral overlays, for Indian enterprises in BFSI, manufacturing and ITes. Book an India Cyber Compliance Workshop. Two hours with your CISO, DPO and risk lead. A gap map across DPDP, CERT-In and your sectoral regulator, plus a costed 2026 build plan in your hands within ten working days.

FAQs

- **When Does the DPDP Act Become Enforceable?**

The DPDP Rules were notified on 13 November 2025. Consent Manager provisions activate on 13 November 2026. Substantive compliance obligations and the penalty regime activate on 13 May 2027.

- **What Is the Maximum DPDP Penalty?**

Up to ₹250 crore (approximately US\$26.24 million) for major violations, imposed by the Data Protection Board after weighing the factors set out in Section 33 of the Act.

- **How Does CERT-In's Six-Hour Clock Interact With DPDP's 72-Hour Clock?**

They run in parallel. CERT-In requires notification of specified incidents within six hours. DPDP requires notification to the Data Protection Board without delay, with a detailed report within 72 hours. The same incident can need to be filed twice, to two regulators, on two different timelines.

- **What Is the SEBI CSCRF?**

The SEBI Cybersecurity and Cyber Resilience Framework, issued in the August 2024 master circular and subsequent clarifications. It applies to 22 categories of SEBI-regulated entities. The 5 May 2026 advisory added an SBOM mandate for critical applications.

- **Who Must Register as a Consent Manager?**

Consent Manager registration opens on 13 November 2026. Only India-incorporated entities with a minimum net worth of ₹2 crore qualify to register. Most Data Fiduciaries will use registered Consent Managers rather than seek registration themselves.

- **Does India Have a Single Cyber Regulator?**

No. DPDP is administered by the Data Protection Board. CERT-In sits under MeitY. NCIIIPC handles critical information infrastructure. RBI, SEBI, IRDAI, DoT and CEA each impose sector-specific obligations. The compliance load is best managed by mapping controls once and reporting many times.

- **What Should an Indian Enterprise Do First in 2026?**

A personal data inventory across all stores. Without it, every other DPDP step is theoretical.

*Published May 2026. Reviewed quarterly against Data Protection Board and sectoral regulator updates.

Proactive Data Systems is an enterprise IT infrastructure and services company. For more than three decades, the company has designed, deployed, and operated the technology foundations behind some of India's most demanding enterprise environments, from regulated industries to large distributed operations.

Founded in 1991, Proactive serves more than 1,500 customers, from fast-growing businesses to Fortune 500 enterprises, across banking and financial services, manufacturing, healthcare, public sector, IT and ITES, retail, education, and global capability centres. Our work spans enterprise networking, cybersecurity, cloud and AI-ready data centres, collaboration platforms, structured cabling, and managed services.

A Cisco Preferred Partner under the Cisco 360 Partner Program, Proactive is recognised across the Networking, Security, Collaboration, Cloud & AI, and Services portfolios, and is a Cisco Advanced Customer Experience Specialised Partner. The company is ISO 9001:2015 and ISO/IEC 27001 certified, and engineers solutions in partnership with Dell, Nutanix, NetApp, Palo Alto Networks, Fortinet, VMware, Veeam, and CommScope.

Headquartered in Delhi NCR, with offices in Mumbai, Bengaluru, Pune, Hyderabad, Indore, and Singapore.

To learn more about our solutions, write to us
at pro@proactive.co.in

 www.proactive.co.in

PROACTIVE™
Enhancing Digital Experience