National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

The Evolving Cybersecurity Regulatory Landscape in India

2025 and Beyond

Table of **Contents**

1

INTRODUCTION

1.1 Purpose & Scope

This report analyzes India's changing cybersecurity regulatory environment up to 2025 and foresees future developments based on emerging trends and policy directions. In the background of fast-paced digitalization and growing cyber threats, India has been gradually building a stronger cybersecurity governance framework. The scope includes major regulatory updates across industries with specific focus on the Digital Personal Data Protection Act (DPDPA) 2023 and Securities and Exchange Board of India's (SEBI) Cyber Security and Cyber Resilience Framework (CSCRF).

The report synthesizes insights from various stakeholders—government, business, security professionals, and civil society—to present a comprehensive picture of how regulatory changes are transforming India's digital landscape. More than a catalog of rules and legislation, this report attempts to reflect the operational implications, compliance issues, and strategic opportunities arising from these regulatory changes.

The intended audience is cybersecurity professionals, compliance officers, business executives, policy researchers, and technology entrepreneurs who want to cut through India's complicated digital regulatory landscape.

1.2 Context & Relevance

India's digital evolution marches at a breakneck speed. Having nearly 900 million internet users in 2024 (Internet in India Report 2024), the world's largest digital democracy comes with special cybersecurity challenges. Several factors make the current regulatory evolution particularly significant:

Global position as an IT service provider, India's increasing effectiveness in adoption and implementation of cybersecurity impacts significantly on supply chains and models of service delivery globally. Organizations worldwide that leverage Indian technology services are now required to understand and account for India's regulatory requirements in their own compliance frameworks.

Second, India's balancing act between security imperatives and digital growth ambitions creates a distinctive regulatory approach that differs from both the European privacy-centric model and the more sectoral American approach. This "third way" is drawing attention from other emerging economies looking to develop their own regulatory frameworks.

The Digital India initiative has dramatically expanded the digital infrastructure, with government services increasingly moving online through platforms like DigiLocker, Aadhaar, and the Unified Payments Interface (UPI). Digitalization of essential services has increased the stakes relating to cybersecurity, transforming regulatory efficacy from an economic concern into a matter of national security and social welfare. Coupled with this ever-growing sophistication of cyber threats is the challenge that media misreporting has added to the high-profile breaches now affecting most institutions: major banks, healthcare providers, and even government agencies, thereby underscoring the more immediate and real consequences of failures in cybersecurity and speeding up the regulation response.

The impact of the COVID-19 pandemic on the long-lasting work patterns with hybrid and remote working models now permanently embedded in the workplace has considerably increased the surface areas for attack as well as extending the boundaries of traditional security perimeters. This has necessitated a review of security requirements for distributed workforces by regulators.

Another level of complexity is added by the geopolitical context. With rising tensions in the region, the critical infrastructure protection has been pushed to the top of regulatory action because of increased cyber activities carried out by state actors. Therefore, India's regulatory responses will have to act against not just criminal threats but also against highly sophisticated nation-state actors.

Against this backdrop, the Digital Personal Data Protection Act and SEBI's enhanced Cyber Security and Cyber Resilience Framework represent milestone developments. Together, they signal India's commitment to a more structured and comprehensive approach to cybersecurity governance.

These frameworks are not merely a reaction to threats that currently bear down on India, but an attempt to proactively build resilience into the digital ecosystem in India. This report therefore occupies a unique position, whereby the first lessons of the initial implementation stages of these critical regulations are being learned, and regulators are gearing up for the next wave of refinements and expansion. The insights presented here aim at assisting organizations not just in compliance but also in leveraging the regulatory necessities to make their digital operations genuinely more secure and resilient.

2

India's Cybersecurity Regulatory Ecosystem

2.1 Legal Framework, Regulators & Key Institutions

India's cybersecurity regulatory framework has come a long way in the last ten years, changing from a patchwork of sectoral guidelines to a more cohesive and systematic ecosystem with clearer governance structures. The IT Act that builds the foundation was amended in the year 2008 to incorporate electronic records, digital signatures, and cybercrime provisions considerably. However, this framework is now supplemented by a range of specialized regulations and institutional mechanisms..

Sectoral Regulators

India's cybersecurity landscape features several sectoral regulators that maintain specialized oversight within their domains while increasingly coordinating their approaches:

Reserve Bank of India (RBI): As the financial sector regulator, the RBI has established some of the most comprehensive cybersecurity frameworks in India. Under the Banking Regulation Act, it issues binding directives for banks and payment systems. The RBI's Cyber Security Framework for Banks (2016, updated in 2023) sets stringent requirements for risk assessment, incident reporting, and security governance. The RBI coordinates with CERT-In on financial sector incident response and participates in cross-sectoral exercises organized by the National Cyber Security Coordinator.

Securities and Exchange Board of India (SEBI): SEBI regulates cybersecurity for stock exchanges, clearing corporations, depositories, and other market infrastructure institutions. Its Cyber Security and Cyber Resilience Framework establishes requirements for these entities and has been progressively expanded to cover broker-dealers and mutual funds. SEBI maintains formal information-sharing protocols with the RBI for addressing vulnerabilities affecting interconnected financial systems.

Insurance Regulatory and Development Authority of India (IRDAI): The IRDAI has developed Guidelines on Information and Cyber Security for Insurers, which establish security governance requirements specific to the insurance sector. The IRDAI participates in the Financial Stability and Development Council's technical group on cybersecurity, which facilitates coordination with other financial sector regulators.

Telecom Regulatory Authority of India (TRAI): TRAI issues recommendations on telecom network security, which are often implemented as license conditions by the Department of Telecommunications. Given the critical nature of telecom infrastructure, TRAI works closely with the NCIIPC on securing telecom networks designated as critical information infrastructure.

Key Institutions

India's cybersecurity governance structure has matured substantially, with clearer delineation of institutional responsibilities:

- **Ministry of Electronics and Information Technology (MeitY)** serves as the nodal ministry for cybersecurity policy development and implementation. It oversees many key cybersecurity initiatives and coordinates the national cybersecurity strategy.

- **Indian Computer Emergency Response Team (CERT-In)** functions as the national agency for incident response. Established under Section 70B of the IT Act, CERT-In has significantly expanded its operational capabilities since 2022. It receives mandatory breach notifications, issues vulnerability alerts, and coordinates incident response across sectors. Its April 2022 directions mandating extensive logging requirements and rapid (6-hour) incident reporting marked a significant expansion of its regulatory footprint.

- **National Critical Information Infrastructure Protection Centre (NCIIPC)** operates under the National Technical Research Organisation (NTRO) to protect designated critical information infrastructure across sectors including energy, finance, transportation, and government services. The NCIIPC has developed detailed sectoral security guidelines and conducts regular security assessments of critical systems.

- **Data Protection Board of India (DPBI)**, constituted under Section 18[1] of the Digital Personal Data Protection Act, 2023, adjudicates disputes where platforms fail to fulfil their obligations in handling personal data. Upon receiving notice of a breach, it can mandate urgent remedial measures, conduct investigations, impose financial penalties, refer complaints for alternative dispute resolution, and accept voluntary undertakings from Data Fiduciaries. The Board also advises the government on blocking repeat offenders, determines whether an inquiry is warranted, and holds authority to penalize violations under the Act. (CURRENTLY BEING SETUP)

- **Office of the National Cyber Security Coordinator (NCSC)** under the Prime Minister's Office coordinates cross-agency cybersecurity efforts and helps harmonize various regulatory initiatives. The NCSC has taken a more visible role in developing the National Cyber Security Strategy and aligning sectoral approaches.

- **Indian Cyber Crime Coordination Centre (I4C)** established by the Ministry of Home Affairs, focuses on cybercrime investigation and prevention. With seven components including the National Cyber Crime Threat Analytics Unit and the National Cyber Crime Reporting Portal, I4C has become increasingly important in addressing the law enforcement aspects of cybersecurity.

This ecosystem of institutions is changing continuously, with better coordination across departments through the joint working groups on cybersecurity, and regular consultative forums with public and private stakeholders. The ongoing operationalization of the National Cyber Security Strategy 2023 has further clarified institutional mandates and coordination mechanisms, though some jurisdictional overlaps remain a challenge for regulated entities navigating multiple compliance obligations.

2.2 Major Policies & Guidelines

India's cybersecurity policy landscape has undergone significant transformation, with several key developments shaping the current regulatory environment:

National Cyber Security Policy and Strategy

National Cyber Security Policy 2013 was the first comprehensive cybersecurity policy framework in India. This policy framework aims at protection of critical infrastructure, public-private partnerships and creating security awareness etc.The 2023 National Cyber Security Strategy is a more comprehensive, threat-informed document that has clearer implementation and stewardship mechanisms.

The strategy identifies three pillars: secure (focusing on system security), safe (addressing citizen protection), and resilient (emphasizing business continuity). It establishes more specific targets, including the creation of sectoral Computer Security Incident Response Teams (CSIRTs), the development of an indigenous security technology ecosystem, and enhanced international cooperation mechanisms.

The new strategy brings in the concept of “security by design” as a guiding principle for public and private digital initiatives while calling for security standards in emerging technologies like IoT, AI, and 5G . The strategy presents a unified plan for supply chain security, especially for criticsectors.

Data Protection Framework

Prior to the DPDPA 2023, data protection was primarily governed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These rules established basic requirements for protecting sensitive personal data but lacked comprehensive enforcement mechanisms.

The DPDPA represents a significant evolution, creating a principles-based approach to data protection while establishing the Data Protection Authority as the primary enforcement body.The rules pertaining to security, which specify encryption standards, access control requirements, security vulnerabilities, and testing procedures, are specified in the Data Protection (Technical and Organizational Measures for Data Fiduciaries) Rules, 2023. The rules impose a graded set of security duties, with “significant data fiduciaries” facing heavier obligations like obligatory Data Protection Impact Assessments and independent security review audits. Significant data fiduciaries are classified based on factors like the volume and sensitivity of data, as well as impact.

Sectoral Guidelines

Through different circulars and guidelines such as Cyber Security Framework for Banks (2016, and revised in 2023) Reserve Bank of India has laid down some of the most detailed requirements on cyber security. The 2023 framework update Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices introduced requirements for advanced threat hunting, zero trust architecture implementation, and supply chain risk management for banking entities.

SEBI's Cyber Security and Cyber Resilience Framework (CSCRF), first issued in 2015 and significantly expanded in 2023-24, establishes comprehensive requirements for market infrastructure institutions and other regulated entities. The framework now includes detailed provisions on cloud security, API protection, vulnerability management, and cybersecurity governance at the board level.

The Telecommunications sector operates under the Unified License Agreement's security conditions and TRAI's security directives. The Department of Telecommunications introduced enhanced telecom security requirements in 2023, focusing on network security evaluation, especially for equipment connecting to critical networks.

Healthcare cybersecurity guidelines are emerging under the Digital Information Security in Healthcare Act DISHA. However, the National Digital Health Mission continues to develop specific security standards for health data through its Health Data Management Policy.

Critical Infrastructure Protection

The Critical Information Infrastructure Protection framework, developed by NCIIPC, provides guidance for the protection of systems in sectors characterized as critical. This includes detailed guidance on appropriate security controls, reporting requirements, and resilience planning.

The framework was updated to address emerging threats, with additional emphasis on operational technology security for industrial systems, and stronger requirements for segmentation between IT and OT networks. The update now includes also a maturity model-based approach whereby organizations can assess their security posture against published industry standards.

2.3 Trends & Challenges

Several distinct trends have emerged in India's cybersecurity regulatory landscape, accompanied by significant implementation challenges that organizations must navigate.

Regulatory Convergence

With respect to harmonization, it is the increasing convergence of sectoral cybersecurity regulations. Where earlier regulatory schemes were developed largely in isolation, creating contradictory compliance requirements that overlapped each other, the last few years have seen more cross-sectoral consistency. For example, the banking sector will have to reconcile the incident-reporting obligations set forth by the RBI, being 6 hours, same as CERT-In directives, which provide for a six-hour window. The National Cyber Security Strategy served to fast-track the convergence across different domains by establishing some common principles of cybersecurity that would be relevant to the respective regulations.

The alignment here, however, is seen between the security provisions of the DPDPA and the sectoral security requirements prescribed by the regulators like the RBI and SEBI. This is further evidenced by the increasing adoption of common security frameworks, like the NIST CSF and ISO 27001, as associated reference points across these same regulatory directions.

Hpwever the convergence is not yet complete, Organizations that operate across multiple sectors will still find themselves facing divergent reporting timelines, documentation requirements, and specifications on security controls.

Risk-based Regulation

Another significant trend is the shift from prescriptive, checkbox-style compliance requirements toward risk-based approaches. Recent regulatory updates increasingly focus on organizational risk assessment processes rather than uniform security measures. This approach acknowledges that different organizations face different threat landscapes based on their sector, size, and the sensitivity of data they handle.

SEBI's 2024 CSCRF updates exemplify this trend, requiring regulated entities to develop risk-based cybersecurity programs proportionate to their specific operational contexts. Similarly, the DPDPA establishes different security obligations for significant data fiduciaries based on the risk profile of their data processing activities.

This risk-based approach theoretically allows for more efficient allocation of security resources. However, it also creates implementation challenges, as organizations must develop sophisticated risk assessment methodologies and demonstrate their effectiveness to regulators. Smaller organizations often struggle with this requirement, lacking the expertise to conduct comprehensive risk evaluations.

Localization Requirements

Data localization continues to be a complex regulatory trend with significant cybersecurity implications. While the DPDPA relaxed some earlier proposed restrictions on data transfers, it maintains rigorous requirements for critical personal data and establishes a white-list approach for permissible cross-border transfers.

Similar localization trends appear in sectoral regulations. The RBI's 2018 directive requiring storage of payment data in India remains in force, complemented by additional requirements for financial institutions using cloud services. The Electronic Medical Records Standards similarly impose constraints on health data storage locations.

These localization requirements create significant operational challenges for multinational organizations and cloud service providers. Many companies have responded by developing India-specific data architectures, often involving local data centers or hybrid cloud arrangements. This fragmentation of data environments can itself introduce security vulnerabilities if not carefully managed.

Compliance Burden and Capacity Challenges

The proliferation of cybersecurity regulations has substantially increased compliance burdens, particularly for multi-sector organizations. A mid-sized financial institution operating across India might now face compliance obligations from more than ten different regulatory directives, each with its own reporting and documentation requirements.

This regulatory expansion has outpaced the growth of cybersecurity expertise in India. The country faces an estimated shortage of 500,000 cybersecurity professionals in 2025, making compliance particularly challenging for smaller organizations without dedicated security teams. This skills gap affects both private sector implementation and regulatory enforcement capacity.

Regulators have responded to these capacity challenges through various initiatives, including the CERT-In empaneled security auditor program, which certifies security professionals qualified to conduct regulatory compliance assessments. However, these programs have not yet scaled sufficiently to meet market demand.

Incident Disclosure Tensions

Mandatory breach notification requirements have expanded dramatically, with CERT-In, DPDPA, and sectoral regulators all imposing disclosure obligations with varying timelines and thresholds. These requirements aim to improve transparency and enable coordinated responses to serious incidents.

However, implementation has revealed significant tensions. Organizations report difficulty in meeting aggressive notification timeframes (ranging from 2 to 72 hours depending on the regulation) while simultaneously managing active security incidents. Early notifications often contain incomplete or inaccurate information, creating both regulatory compliance risks and potential reputation management challenges.

Technology-specific Regulatory Challenges

Emerging technologies continue to create regulatory challenges, as existing frameworks struggle to address novel risk profiles:

- **Cloud security regulations** remain fragmented, with different approaches across government procurement guidelines, financial sector requirements, and critical infrastructure protection frameworks. The cloud security assessment model introduced by CERT-In in late 2023 represents an attempt to harmonize these approaches, but implementation remains inconsistent.

- **IoT security** presents particular challenges for the regulatory framework, as responsibilities span device manufacturers, service providers, and network operators. The Telecommunications Standards Development Society of India has developed IoT security standards, but enforcement mechanisms remain limited.

- **AI governance frameworks** have begun to emerge, including NITI Aayog's Responsible AI guidelines and MeitY's national strategy for AI. However, these have yet to translate into comprehensive security requirements for AI systems, leaving significant ambiguity around obligations for secure AI development and deployment.

- **Blockchain applications** face regulatory uncertainty, with cryptocurrency regulations in flux and broader distributed ledger applications operating in a legal gray area regarding data protection obligations. The proposed Digital India Act may clarify some of these issues, but its final form remains uncertain.

Public-Private Collaboration Dynamics

Recent years have seen significant enhancement of public-private partnership mechanisms in cybersecurity regulation. The Joint Working Group on cybersecurity policy has successfully integrated industry representatives from key sectors, fostering collaborative approach to policy development. Both CERT-In and NCIIPC have established productive private sector advisory committees that facilitate information sharing and practical implementation strategies.

These partnerships have yielded tangible benefits for the cybersecurity ecosystem. Industry participation has helped develop more implementable technical standards and realistic compliance timelines. Meanwhile, government agencies have gained deeper insights into emerging threats and sector-specific vulnerabilities.

As India's cybersecurity regulatory landscape continues to mature, these collaborative approaches will become increasingly important for developing adaptive, effective security frameworks that balance robust protection with practical implementation considerations.

3

Case Study I: Digital Personal Data Protection Act (DPDPA)

3.1 Core Provisions

The Digital Personal Data Protection Act (DPDPA), enacted in 2023, represents India's most significant data protection legislation to date. After several years of draft bills and public consultations, the DPDPA establishes a comprehensive framework that balances individual rights with business needs while creating substantial cybersecurity obligations. Its core provisions include:

Scope and Jurisdiction

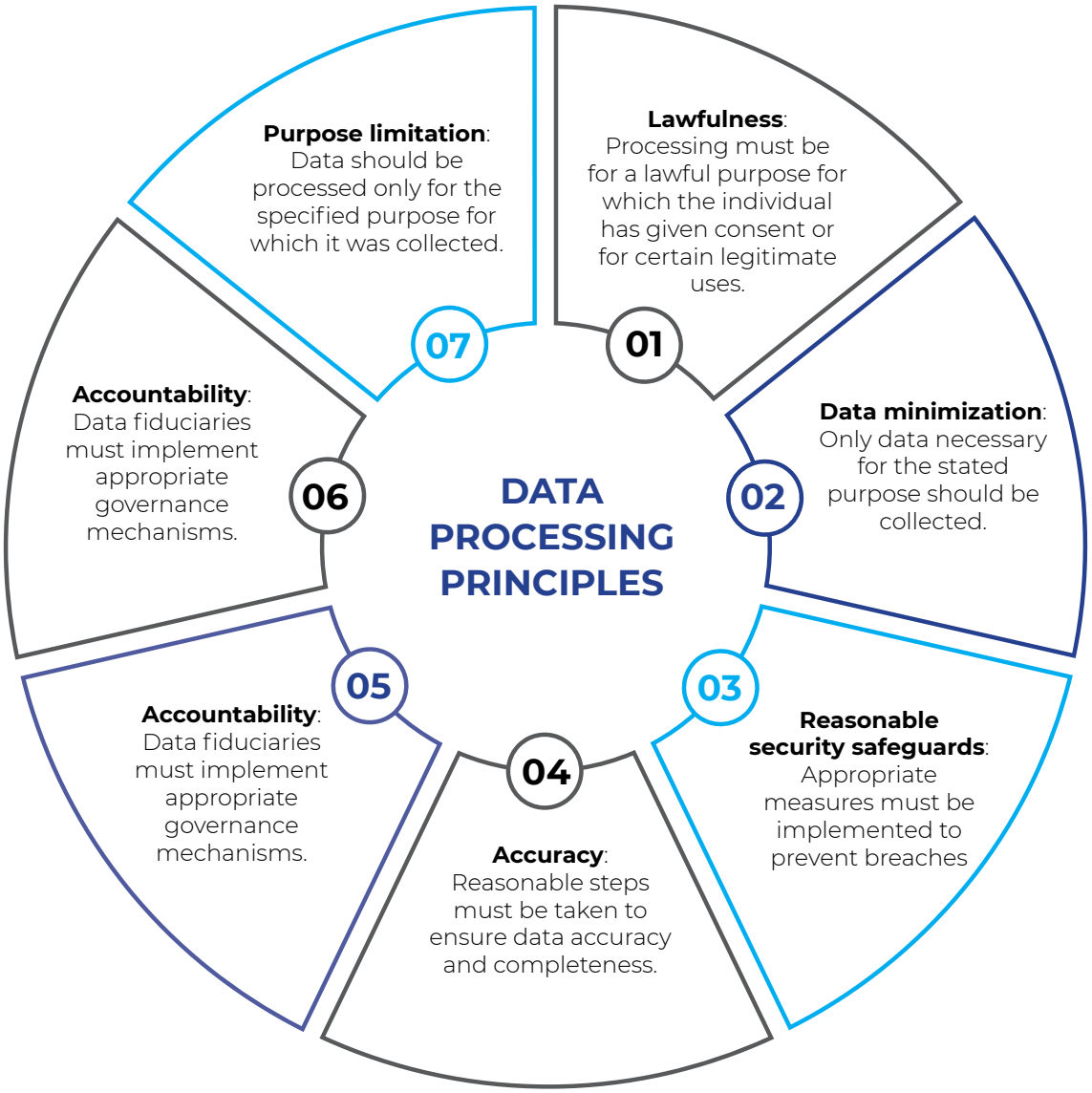
The DPDPA applies to the processing of digital personal data within Indian territory, regardless of whether the processing entity is based in India. It also extends to data processing outside India if connected to offering

goods or services to individuals in India or profiling their behavior. This extraterritorial scope mirrors approaches seen in the EU's GDPR but with some India-specific adaptations.

Notably, the Act excludes non-automated processing, data processing by individuals for personal or domestic purposes, and data contained in records at least 50 years old. It applies different standards to government agencies—an approach that has drawn criticism from privacy advocates.

Data Processing Principles

The DPDPA establishes seven fundamental principles for data processing:



These principles create the foundation for the Act's more specific requirements and establish a principles-based approach that allows for flexibility in implementation while maintaining core protections.

Consent Framework

The DPDPA establishes consent as the primary lawful basis for processing personal data, though with significant exceptions. The Act requires that consent be:

- Free, specific, informed, unconditional, and unambiguous
- Indicated through clear affirmative action
- Capable of being withdrawn as easily as it was given

The Act also introduces the concept of "deemed consent" for various processing activities including compliance with legal obligations, medical emergencies, public interest purposes, and employment-related processing. This approach differs from the GDPR's multiple lawful bases and has raised concerns about potential overreliance on deemed consent provisions.

Individual Rights

The DPDPA grants data principals (individuals) several enforceable rights:

- Right to information about data processing
- Right to access and correction
- Right to data portability
- Right to erasure of personal data
- Right to grievance redressal
- Right to nominate another person to exercise rights after death

Notably absent is the right to object to processing (beyond withdrawing consent) and the right against automated decision-making, which appear in some other global privacy frameworks.

Data Fiduciary Obligations

Organizations processing personal data (termed "data fiduciaries") face various obligations:

- Implementing appropriate security safeguards against unauthorized access, disclosure, or destruction of data

- Establishing effective data breach response procedures
- Maintaining transparency through clear privacy notices
- Conducting Data Protection Impact Assessments for high-risk processing
- Appointing Data Protection Officers for significant data fiduciaries
- Ensuring that third-party processors comply with security requirements

The security safeguards requirement is particularly significant from a cybersecurity perspective, as it establishes an affirmative obligation to implement appropriate technical and organizational measures. The subsequent Technical and Organizational Measures Rules provide more specific guidance on these requirements.

Cross-Border Data Transfers

The DPDPA adopts a more flexible approach to cross-border transfers than earlier drafts, permitting transfers to countries or territories specified by the government. This whitelist approach differs from both the earlier proposed data localization requirements and the GDPR's adequacy decision model.

The Act empowers the government to restrict transfers to specific countries based on relevant factors including security considerations. Notably, it maintains separate rules for "critical personal data," which must be processed only in India, though this category has yet to be fully defined.

Reporting and Compliance

The Act establishes significant compliance mechanisms:

- Mandatory notification of personal data breaches to the Data Protection Board and affected individuals
- Annual compliance reporting for significant data fiduciaries
- Independent data protection audits conducted by certified auditors
- Registration requirements for significant data fiduciaries

The breach notification requirement is particularly noteworthy, though the specific timelines and thresholds were left to subsequent rules rather than specified in the Act itself.

Enforcement and Penalties

The DPDPA creates a Data Protection Board of India with investigation and enforcement powers. Administrative penalties for violations can reach

up to ₹250 crore (approximately $30 million) or 4% of global turnover for serious violations. This represents a substantial increase in potential financial consequences compared to the previous IT Act provisions.

The Act also creates a unique framework for voluntary undertakings, allowing organizations to propose remedial measures in response to potential violations. This mechanism potentially offers a more collaborative enforcement approach compared to purely punitive measures.

These core provisions reflect India's attempt to create a balanced framework that addresses privacy and security concerns while accommodating practical business needs. While drawing inspiration from international frameworks like the GDPR, the DPDPA incorporates distinctly Indian elements, creating unique compliance challenges for organizations operating in the Indian market.

3.2 Impact on Stakeholders

Stakeholder	Key Observations & Impacts
For Businesses	**Large Corporations**: Multinational enterprises and large Indian conglomerates generally leveraged existing GDPR-style compliance programs, but had to adapt for Indian-specific nuances (e.g., deemed consent, fiduciary obligations). Financial institutions faced added complexity harmonizing DPDPA with RBI guidelines, incurring additional implementation costs. Tech giants (Google, Meta, Amazon) reorganized data flows and consent processes specifically for India, submitting formal feedback during rule-making. **Small & Medium Enterprises (SMEs)**: Many struggled due to limited resources and expertise. A 2024 NASSCOM survey showed only 47% felt adequately prepared. The Act's security requirements drove demand for managed security service providers (MSSPs), which grew ~35% in 2024. Associations like CII, FICCI, NASSCOM, and the Ministry of MSMEs offered toolkits and awareness programs. **Startups**: For data-heavy startups, operational costs rose and business models sometimes required changes, with VCs now factoring DPDPA compliance in due diligence. Simultaneously, privacy-tech startups saw opportunities, offering compliance software and security solutions.

Stakeholder	Key Observations & Impacts
For Individuals	Surveys indicate moderate awareness (~40% of urban internet users). Access/correction requests are increasingly common, yet portability and erasure remain underutilized. Consent interfaces have become more prominent, sometimes leading to higher user abandonment (by ~12% in e-commerce according to a 2024 Nielsen study). Privacy advocates hail the expanded rights but criticize broad government exemptions and potential overuse of deemed consent.
For Government Entities	Many government digital services required DPDPA-aligned redesign, coordinated by a special MeitY task force. The Central Board of Direct Taxes and UIDAI actively implemented controls, with UIDAI's data governance framework serving as a model for other agencies. Various States are looking to establish dedicated privacy offices, but some state departments face challenge because of budget constraints and overlapping digital priorities.
For Specific Sectors	**Healthcare**: Balances data protection with clinical imperatives. The National Digital Health Mission is adapting DPDPA rules, especially consent management for health data. Large hospital chains adopted specialized HIS (health information systems) with built-in privacy features, while smaller providers struggle with compliance. **Financial Services**: Banks/insurers adapted established data protection measures. Fintechs, reliant on data-sharing models, underwent significant revisions. RBI aligned its cybersecurity circulars with DPDPA to clarify overlaps. **Education**: Implementing parental/guardian consent for minors proved challenging. The University Grants Commission released higher-ed compliance guidelines (late 2023), and EdTech platforms revamped data handling, parental controls, and record management.

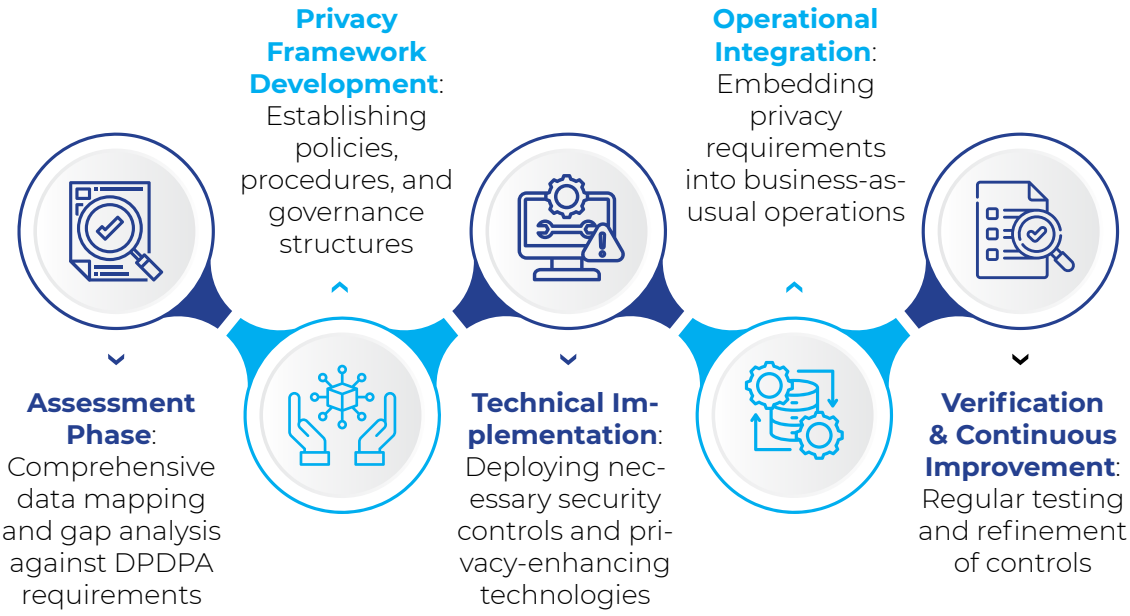
Stakeholder	Key Observations & Impacts
Cross-Border Service Providers	Major cloud vendors introduced India-centric data center footprints and specialized compliance tiers. Global software firms released India-specific privacy modules. International consulting firms saw significant growth—DPDPA-related revenue for such services surpassed ₹5,000 crore (~$625 million) in 2024—helping enterprises translate legal mandates into workable implementation roadmaps.
For Regulators and the Legal System	A new **Data Protection Board** is being setup, focusing on breach notification thresholds and cross-border data transfer mechanisms. The legal profession expanded privacy law specializations, and new data protection certifications emerged (e.g., at National Law School of India University). Courts increasingly invoke DPDPA principles: a Delhi High Court case in Jan 2025 cited its consent standards in a consumer protection ruling, foreshadowing wider judicial adoption of data protection norms.
Overall Outlook	As DPDPA implementation unfolds, compliance processes continue to evolve, and enforcement is still maturing. Nevertheless, the Act has already reshaped how personal data is managed across India's digital ecosystem, creating novel obligations, fresh commercial opportunities, and a new wave of challenges for every stakeholder—from corporations and government agencies to individuals.

3.3 Early Implementation Insights

Since the DPDPA's implementation began in phased rollouts starting in late 2023, organizations have gained valuable insights into effective compliance approaches, common pitfalls, and practical challenges. These early experiences provide important lessons for organizations still building their compliance programs.

Implementation Approaches

Implementation timelines have varied significantly across sectors and organization types. The most successful implementations have typically followed a phased approach:



Regulatory Interpretation and Guidance

Early implementation has been shaped by regulatory guidance issued by the Data Protection Board and other agencies:

The Data Protection Board published its initial interpretative guidance in Q4 2023, addressing key implementation questions including:

- Criteria for designating "significant data fiduciaries"
- Standards for valid consent collection
- Acceptable approaches to data minimization
- Requirements for data protection impact assessments

This guidance helped clarify areas where the legislation's language left room for interpretation. However, several ambiguities remain, particularly regarding cross-border transfer mechanisms and the scope of deemed consent provisions.

Sectoral regulators have issued complementary guidance to help harmonize existing requirements with the DPDPA:

These sectoral guidelines have helped reduce compliance conflicts but have sometimes introduced additional requirements beyond the core DPDPA obligations, creating implementation complexity for multi-sector organizations.

Security Implementation Insights

The DPDPA's security requirements have driven significant investments in cybersecurity capabilities:

- Identity and Access Management (IAM) solutions have seen particularly strong adoption, with organizations implementing stronger authentication controls and more granular access governance. Multi-factor authentication has become standard for systems handling sensitive personal data.
- Data Loss Prevention (DLP) technologies have been widely deployed to monitor and control personal data movements. Organizations have learned to implement these tools gradually, beginning with monitoring modes before enforcing blocking controls, to avoid business disruption.
- Encryption adoption has accelerated, though with implementation challenges. While transit encryption is now nearly universal, at-rest encryption implementation has proven more complex, particularly for legacy systems. Organizations have developed risk-based approaches, prioritizing encryption for the most sensitive data categories.
- Security awareness training programs have been enhanced to incorporate privacy-specific elements. Organizations report that training scenarios built around realistic DPDPA compliance situations have been more effective than generic privacy training.

Successful security implementations have typically aligned DPDPA requirements with existing security frameworks like ISO 27001, NIST CSF, or CIS Controls. This integrated approach has proven more sustainable than creating separate security controls solely for DPDPA compliance.

Some organizations have found unexpected benefits from DPDPA implementation:

- Improved data governance has enhanced data quality and availability for legitimate business purposes
- Enhanced security controls have reduced overall breach risk beyond just personal data
- Privacy-focused brand messaging has resonated positively with certain customer segments

These benefits have partially offset implementation costs, particularly for organizations that approached compliance as a strategic opportunity rather than merely a regulatory obligation.

Emerging Best Practices

Based on implementation experiences to date, several best practices have emerged:

1. **Governance Integration**: The most successful implementations have integrated data protection governance into existing risk management and corporate governance structures rather than creating parallel processes.
2. **Technology Enablement**: Purpose-built privacy technology solutions have generally proven more effective than manual processes or retrofitted generic tools, particularly for rights management and consent orchestration.
3. **Phased Implementation**: Organizations that prioritized high-risk data processing activities for initial implementation achieved better risk reduction per compliance rupee than those attempting to address all requirements simultaneously.
4. **Documentation Discipline**: Maintaining comprehensive documentation of compliance decisions and rationales has proven valuable, particularly when addressing regulatory questions or adapting to evolving interpretations.
5. **Automation of Routine Tasks**: Organizations that invested in automating routine compliance tasks like data subject request handling and consent management have achieved more sustainable compliance operations than those relying primarily on manual processes.

As implementation continues across the Indian economy, these lessons continue to evolve. The Data Protection Board has indicated plans to publish detailed case studies and compliance guidance based on early implementation experiences, which should further enhance organizational understanding of effective approaches.

4

Case Study II: SEBI Cybersecurity Guidelines

4.1 SEBI's Role & Mandate

The Securities and Exchange Board of India (SEBI) occupies a central position in India's financial regulatory architecture, with a mandate that encompasses investor protection, market development, and the promotion of fair and efficient markets. Established by the SEBI Act of 1992, the regulator has evolved significantly in its approach to cybersecurity, reflecting the growing digitalization of India's financial markets.

Regulatory Authority and Jurisdiction

SEBI's regulatory purview extends across a diverse ecosystem of market entities:

- Stock exchanges (NSE, BSE, and others)
- Clearing corporations and depositories

- Intermediaries including brokers, merchant bankers, and portfolio managers
- Asset management companies and mutual funds
- Credit rating agencies
- Investment advisors and research analysts
- Listed companies and their disclosures

This broad jurisdiction gives SEBI substantial influence over cybersecurity practices across India's financial sector, affecting thousands of entities and indirectly impacting millions of investors.

SEBI derives its cybersecurity regulatory authority from multiple legislative sources:

- The SEBI Act, 1992, which empowers it to regulate securities markets
- The Securities Contracts (Regulation) Act, 1956
- The Depositories Act, 1996
- Various SEBI Regulations issued under these statutes

These instruments collectively allow SEBI to establish binding cybersecurity requirements for regulated entities through circulars, guidance, and regulatory actions.

Evolution of SEBI's Cybersecurity Focus

SEBI's cybersecurity regulatory approach has undergone several phases of development:

Initial Phase (2000-2013): SEBI's early cybersecurity requirements were relatively limited, focusing primarily on basic IT controls for exchanges and clearing corporations. The 2005 "Risk Management System at the Stock Exchanges" circular introduced preliminary requirements for system controls and business continuity.

Framework Development (2014-2018): Recognizing growing cyber threats, SEBI established its first comprehensive Cyber Security and Cyber Resilience Framework in 2015 (Circular CIR/MRD/DP/13/2015). This framework, initially applicable to Market Infrastructure Institutions (MIIs), established baseline requirements across governance, assessment, protection, monitoring, response, and recovery domains.

The framework was gradually extended to additional entity types:

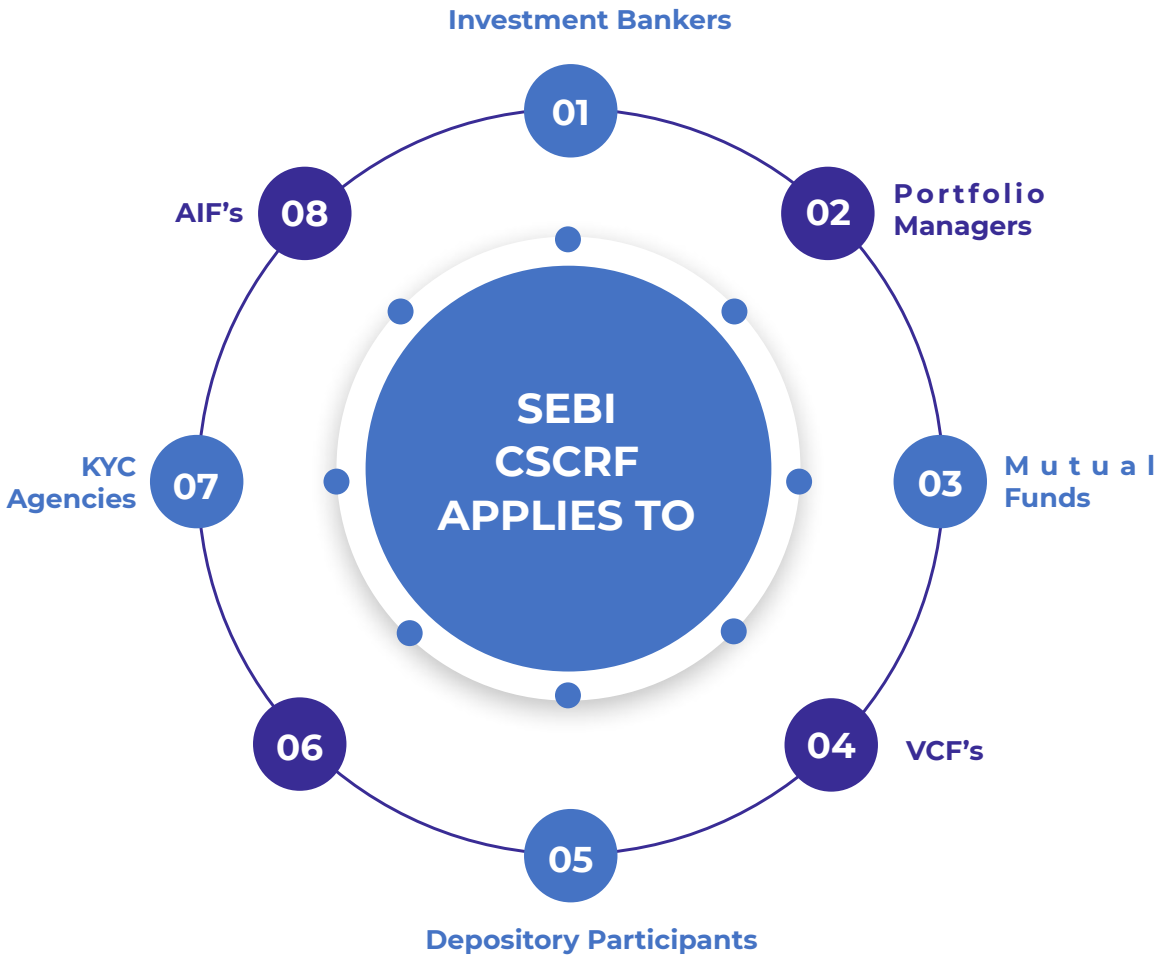
- 2016: Application to clearing corporations and depositories
- 2018: Extension to larger stock brokers and depositories participants
- 2019: Application to mutual funds, asset management companies, and registrar and transfer agents

Maturity and Expansion Phase (2019-2022): During this period, SEBI refined its requirements through periodic updates and entity-specific guidance. The regulator began conducting thematic inspections focused specifically on cybersecurity compliance, signaling increased enforcement focus.

The 2019 update (Circular CIR/MRD/CSC/148/2018) introduced more specific requirements for security operations centers, threat intelligence, and advanced detection capabilities. It also strengthened governance requirements, mandating board-level oversight of cybersecurity risks.

Current Phase (2023-Present): The most recent evolution began with SEBI's comprehensive update to the Cyber Security and Cyber Resilience Framework in 2023 (SEBI/HO/MIRSD/TPD/P/CIR/2023/008). This update significantly expanded requirements, introducing controls for cloud security, API protection, and supply chain risk management.

The current framework applies to an expanded range of entities and incorporates more sophisticated security concepts drawn from global standards including NIST CSF, ISO 27001, and financial sector frameworks. It represents SEBI's most mature and comprehensive approach to date.



Regulatory Philosophy

SEBI's cybersecurity regulatory philosophy emphasizes several core principles:

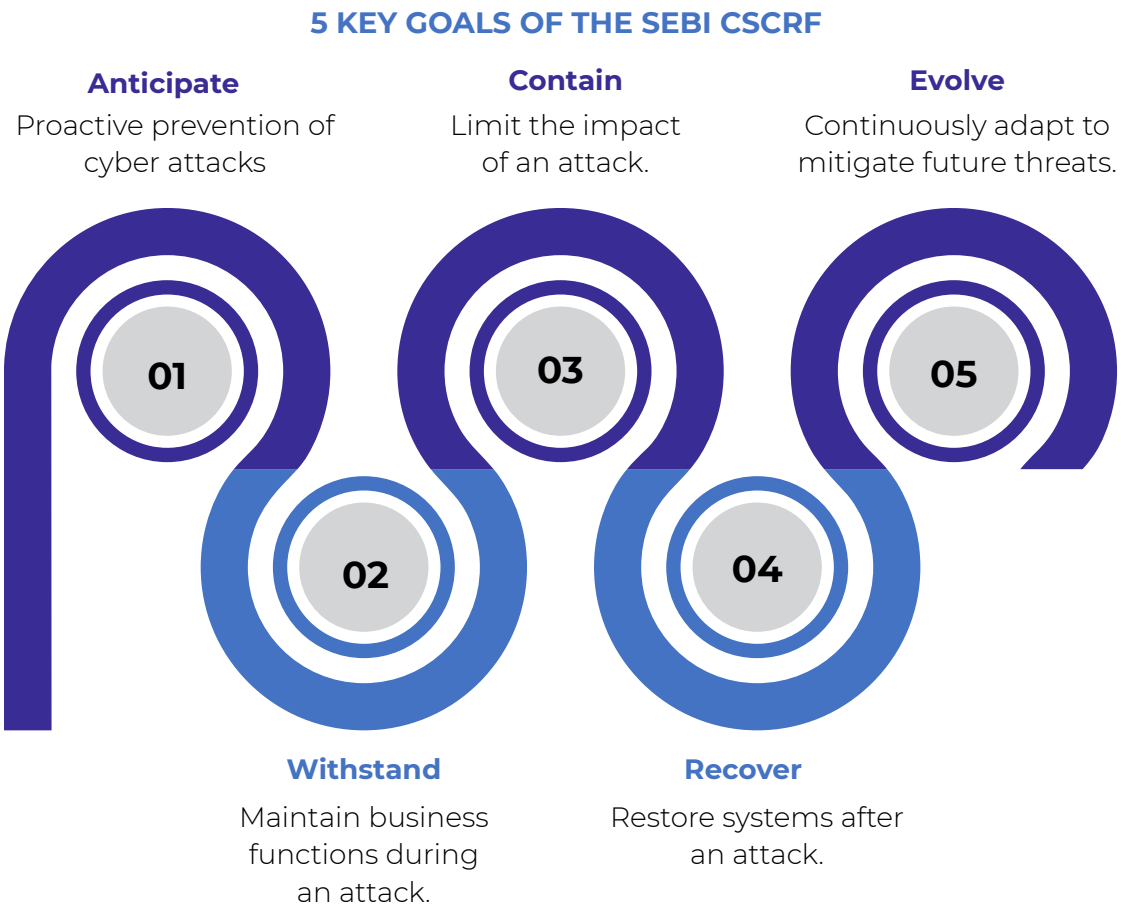
Risk-based Approach: Rather than prescribing uniform controls for all entities, SEBI has increasingly adopted a risk-based approach that calibrates requirements based on an entity's systemic importance, size, and risk profile. This is evident in the tiered implementation timelines and differentiated requirements for entities of varying sizes.

Critical Infrastructure Protection: SEBI places particular emphasis on securing the core market infrastructure, recognizing that exchanges, clearing corporations, and depositories represent potential single points of failure for the broader financial system.

Governance Focus: SEBI consistently emphasizes senior leadership accountability for cybersecurity, requiring board-level oversight and regular reporting. This governance emphasis reflects recognition that effective cybersecurity requires organizational commitment beyond technical controls.

Continuous Evolution: The regulator's approach has been characterized by regular updates to address emerging threats and technologies. SEBI has demonstrated willingness to refine requirements based on implementation experience and evolving risk landscapes.

Collaborative Engagement: SEBI maintains ongoing dialogue with regulated entities through its advisory committees, industry consultations, and periodic workshops. This collaborative approach helps ensure that requirements remain practical and aligned with industry capabilities.



Current Organizational Structure

SEBI's cybersecurity regulatory function is primarily housed within its Information Technology Department (ITD) and Market Intermediaries Regulation and Supervision Department (MIRSD). The ITD focuses on technical standards and system assessments, while MIRSD handles compliance monitoring and enforcement.

The regulator has established specialized capabilities including:

- A dedicated Cyber Security Cell that monitors cyber threat intelligence relevant to securities markets
- A Security Operations Center monitoring SEBI's own systems and coordinating with regulated entities during major incidents
- A Technology Advisory Committee that includes external experts who provide input on cybersecurity regulations

SEBI coordinates closely with other financial regulators through the Financial Stability and Development Council (FSDC) and its technical committee on cybersecurity. This cross-regulatory coordination has become increasingly important as financial entities often fall under multiple regulatory jurisdictions.

SEBI also participates in international regulatory forums including the International Organization of Securities Commissions (IOSCO) Cyber Task Force, which helps align its approach with global best practices.

As cyber threats to financial markets continue to evolve, SEBI's role in cybersecurity governance has grown increasingly central to India's financial stability architecture. The regulator continues to refine its approach based on emerging threats, technological developments, and implementation experience.

4.2 Key Guidelines & Requirements

SEBI's Cyber Security and Cyber Resilience Framework (CSCRF) has evolved into a comprehensive set of requirements addressing diverse aspects of cybersecurity. The most recent major update in 2023, with subsequent clarifications in 2024, establishes detailed expectations across several critical domains:

Governance Requirements

The framework places strong emphasis on governance structures and leadership accountability:

- **Board Oversight**: Boards of regulated entities must approve cybersecurity policies, review implementation status quarterly, and ensure adequate resource allocation. Board members must receive regular cybersecurity awareness training.

- **Chief Information Security Officer (CISO)**: Entities must designate a sufficiently senior CISO with direct reporting access to the board or relevant committee. The CISO must have formal security qualifications and relevant experience. For smaller entities, this role may be outsourced to qualified professionals, subject to specific oversight requirements.
- **Information Security Committee**: Larger entities must establish cross-functional information security committees including representatives from technology, business, risk, and compliance functions. This committee typically meets monthly to oversee implementation and address emerging risks.
- **Policy Framework**: Entities must maintain board-approved information security policies addressing all major control domains. These policies must be reviewed at least annually and updated based on risk assessments and incident learnings.
- **Security Strategy**: Regulated entities must develop and maintain a multi-year cybersecurity strategy aligned with business objectives and emerging threats. This strategy must be reviewed annually and must include measurable security objectives.

Risk Management Requirements

Risk assessment forms the foundation of SEBI's framework:

- **Comprehensive Risk Assessment**: Entities must conduct formal cybersecurity risk assessments at least annually, covering systems, applications, networks, and third-party services. The methodology must align with recognized standards such as NIST 800-30 or ISO 27005.
- **Continuous Vulnerability Assessment**: Larger entities must implement continuous vulnerability scanning programs covering all internet-facing assets. Critical vulnerabilities must be remediated according to defined timelines based on risk level.
- **Penetration Testing**: Independent penetration tests must be conducted at least annually for internet-facing systems and critical internal systems. Tests must be conducted by qualified third parties or adequately segregated internal teams.
- **Application Security**: Security testing must be integrated into application development lifecycles, with formal secure coding standards and pre-deployment security reviews. Dynamic application security testing is required for all customer-facing applications.

- **Risk Register**: Entities must maintain a formal cybersecurity risk register documenting identified risks, mitigation measures, residual risk levels, and accountable owners. This register must be reviewed quarterly by senior management.

Technical Security Requirements

The framework specifies detailed technical controls across multiple domains:

- **Network Security**: Requirements include network segmentation based on data sensitivity, intrusion detection/prevention systems, regular network vulnerability assessments, secure network architecture reviews, and strong controls for remote access.
- **Access Management**: The framework mandates implementation of the principle of least privilege, multi-factor authentication for administrative access, privileged access management solutions, formal user access reviews, and strong password policies.
- **Data Protection**: Requirements include data classification based on sensitivity, encryption for sensitive data in transit and at rest, database activity monitoring, data loss prevention controls, and secure data disposal procedures.
- **Endpoint Security**: Mandated controls include endpoint protection platforms, centralized patch management, device encryption, application whitelisting for critical systems, and mobile device management for corporate devices.
- **Cloud Security**: The 2023 update introduced specific requirements for cloud security, including mandatory risk assessments for cloud services, contractual security requirements for cloud providers, cloud access security brokers for larger entities, and continuous security monitoring of cloud resources.
- **API Security**: Reflecting the growing importance of APIs in financial services, the framework now requires API security gateways, formal API inventory management, API authentication standards, and rate limiting for public APIs.
- **Cryptography**: Requirements include cryptographic key management procedures, regular rotation of encryption keys, use of industry-standard encryption algorithms, and secure storage of cryptographic material.

Detection and Response Requirements

The framework places strong emphasis on threat detection and incident response capabilities:

- **Security Monitorin**g: Larger entities must maintain 24x7 security operations centers (SOCs), either in-house or through managed security service providers. The SOC must monitor security events from critical systems, investigate alerts based on defined procedures, and maintain defined service levels for alert triage.
- **Threat Intelligence**: Entities must participate in information sharing communities, subscribe to relevant threat intelligence feeds, and incorporate intelligence into detection and prevention measures. Market Infrastructure Institutions must establish capabilities to analyze and disseminate threat intelligence to participants.
- **Incident Response**: Requirements include documented incident response plans, regular testing through tabletop exercises, defined escalation procedures, and post-incident reviews. The framework specifies maximum response time objectives for different incident severity levels.
- **Breach Reporting**: Significant cybersecurity incidents must be reported to SEBI within 6 hours of detection, with subsequent detailed reports within 24 hours and 72 hours. Critical incidents affecting market operations require immediate notification.
- **Forensic Readiness**: Larger entities must maintain forensic investigation capabilities, either in-house or through pre-arranged service provider relationships. System logging must support forensic investigation requirements.

Resilience Requirements

Business continuity and recovery capabilities form a key component of the framework:

- **Recovery Planning**: Entities must establish recovery time objectives and recovery point objectives for critical systems based on business impact analysis. These objectives must be validated through regular testing.
- **Backup Management**: The framework mandates air-gapped backups for critical systems, regular backup testing, and encryption of backup data. Backup restoration processes must be tested at least semi-annually.
- **Disaster Recovery**: Regulated entities must maintain disaster recovery sites with appropriate geographical separation from primary sites. Larger entities must implement near-real-time data replication for critical systems.

Recovery capabilities must be tested through full-scale exercises at least annually.

- **Cyber Resilience Assessment**: Entities must regularly assess their overall cyber resilience using scenario-based testing and must develop improvement plans based on assessment results.
- **Destructive Attack Preparedness**: The 2023 update added specific requirements for preparedness against destructive attacks including ransomware, requiring segmented recovery capabilities and offline recovery procedures.

Third-Party Risk Management

The framework includes extensive requirements for managing supply chain and vendor risks:

- **Due Diligence**: Entities must conduct security due diligence before engaging critical technology service providers. This assessment must include review of the provider's security controls, past incidents, and compliance certifications.
- **Contractual Requirements**: Contracts with technology service providers must include specific security requirements, right-to-audit provisions, incident notification obligations, and service level agreements for security-related performance.
- **Ongoing Monitoring**: Entities must establish programs for continuous monitoring of third-party security posture, including periodic reassessments, vulnerability disclosure requirements, and tracking of sub-contractor relationships.

- **Exit Planning**: Contracts must address secure transition arrangements in case of service termination, including data return or secure destruction procedures and knowledge transfer requirements.

Implementation Requirements

The framework establishes specific requirements for implementation and compliance verification:

- **Independent Assessment**: Regulated entities must undergo independent cybersecurity assessments at least annually. These assessments must be conducted by qualified third parties or adequately segregated internal audit functions.
- **Reporting**: Assessment results must be reported to the entity's board and SEBI within defined timeframes. Remediation plans for identified deficiencies must be developed and tracked to completion.
- **Awareness and Training**: All employees must receive cybersecurity awareness training at least annually. Technical staff must receive role-specific security training. Both programs must be refreshed regularly to address emerging threats.
- **Continuous Improvement**: Entities must establish formal processes for tracking and implementing security improvements based on incidents, assessment findings, and emerging threats.
- The framework includes implementation timelines that vary based on entity size and criticality. Market Infrastructure Institutions face the most stringent timelines, while smaller intermediaries receive extended implementation periods for more complex requirements.
- SEBI's approach combines principles-based requirements with specific technical controls, creating a comprehensive framework that aims to address the diverse cybersecurity challenges facing India's financial markets. The framework continues to evolve, with SEBI indicating plans for further refinements focused on emerging technologies including AI systems, quantum-resistant cryptography, and distributed ledger applications.

4.3 Sectoral Challenges & Best Practices

- The implementation of SEBI's Cyber Security and Cyber Resilience Framework (CSCRF) has revealed unique sectoral challenges and spawned innovative responses across India's diverse securities market ecosystem. These experiences provide valuable insights for organizations working to enhance their cybersecurity posture under regulatory requirements.

Market Infrastructure Institutions (MIIs)

- Stock exchanges, clearing corporations, and depositories—collectively known as Market Infrastructure Institutions—form the critical core of India's securities markets. These entities face unique cybersecurity challenges:

Challenges

- **High Availability Requirements**: MIIs must maintain near-continuous operations, making traditional security maintenance windows problematic. The National Stock Exchange operates with 99.999% uptime targets, creating tension between security patching and availability requirements.
- **Interconnected Ecosystem Risks**: MIIs operate within a highly interconnected technical ecosystem, with complex dependencies on telecommunication providers, data centers, and market participants. The 2021 incident where a telecom provider misconfiguration affected NSE operations highlighted these interconnection risks.
- **Advanced Threat Landscape**: As critical financial infrastructure, MIIs face sophisticated threats including nation-state actors. The BSE reported a 300% increase in advanced persistent threat attempts between 2022 and 2024.
- **Legacy Technology Integration**: Many core trading and settlement systems incorporate legacy components developed decades ago, creating security modernization challenges. The transition to T+1 settlement in 2022 required significant security architecture adjustments to maintain appropriate controls during accelerated processing timeframes.

Emerging Best Practices:

MIIs have developed several innovative approaches to address these challenges:

- **Active-Active Security Architecture**: Leading exchanges have implemented active-active security infrastructure that allows security components to be updated without service interruption. This approach enables continuous security improvement without compromising availability.
- **Participant Security Programs**: Recognizing ecosystem risks, MIIs have established formal programs to enhance the security posture of connected

participants. The NSE's Member Security Enhancement Initiative includes security assessment frameworks, technical guidelines, and periodic security workshops for members.

- **Advanced Threat Hunting**: Major MIIs have established dedicated threat hunting teams that proactively search for indicators of compromise using advanced analytics. These teams supplement traditional security monitoring with hypothesis-driven investigation techniques.
- **Secure Modernization Frameworks**: Several MIIs have developed structured approaches for secure technology modernization that address legacy system risks. These frameworks include specialized security testing for legacy interfaces and enhanced monitoring during transition periods.
- The Securities Industry Risk Group established by major MIIs in 2023 provides a forum for sharing security practices and coordinating responses to sector-wide threats. This collaborative approach has enhanced the overall resilience of market infrastructure.

Trading Members and Brokers

- The broker community presents particularly diverse cybersecurity challenges, with entities ranging from large national firms to small regional operators:

Challenges

- **Resource Disparities**: Smaller brokers often lack dedicated security personnel and operate with limited technology budgets. A 2024 Association of National Exchanges Members of India (ANMI) survey found that 62% of small brokers had no full-time security staff.
- **Digital Transformation Pressure**: Competitive pressure to provide sophisticated digital trading experiences has accelerated technology adoption, sometimes outpacing security controls. Mobile trading applications developed under compressed timeframes have been particularly vulnerable to security issues.
- **Client-side Vulnerabilities**: Brokers face significant challenges securing the client environment, with retail traders often using inadequately protected personal devices. The 2023 Operation Gold Rush incident, where thousands of retail trading accounts were compromised through credential theft, highlighted these client-side risks.
- **Regulatory Overlap**: Many brokers must simultaneously comply with requirements from multiple regulators including SEBI, RBI (for banking services), and IRDAI (for insurance distribution), creating compliance complexity.

Emerging Best Practices:

The broker community has developed several effective approaches:

- **Security Service Models**: Industry associations have facilitated the development of shared security service models that allow smaller brokers to access sophisticated security capabilities through consortium arrangements. The ANMI Security Operations Center provides managed security services specifically tailored to smaller brokers' needs.
- **Progressive Security Implementation**: Successful brokers have adopted phased implementation approaches that prioritize critical controls addressing the most significant risks. This risk-based approach allows for efficient use of limited security resources.
- **Client Security Enablement**: Leading brokers have invested in client security awareness programs and technical controls to enhance end-user protection. These include simplified security guidance, suspicious activity notifications, and optional enhanced security features like hardware security keys.
- **Compliance Harmonization Frameworks**: Larger brokers with multi-regulatory obligations have developed mapping frameworks that identify control overlaps across different regulatory requirements, enabling more efficient implementation and compliance demonstration.
- The establishment of the Brokers Security Forum in 2023 has created an avenue for security knowledge sharing among brokers of all sizes, helping raise the overall security maturity of the sector.

Asset Management Companies (AMCs)

Mutual fund operators and other asset management entities face distinct cybersecurity challenges:

Challenges

- **Data Sensitivity Concentration**: AMCs manage highly sensitive investor data including KYC information, financial holdings, and transaction histories. The comprehensive nature of this data makes it particularly attractive to attackers.
- **Complex Partner Ecosystem**: AMCs typically operate through extensive networks of distributors, registrars, and transfer agents, creating a complex web of data sharing relationships. A 2023 incident where a distributor's compromise led to data exposure for multiple AMCs highlighted these ecosystem risks.
- **Insider Threat Risks**: The nature of asset management creates elevated insider risk potential, with employees having access to market-sensitive information and customer assets. Detection of malicious insider activity requires specialized controls beyond traditional security measures.
- **Hybrid Infrastructure Models**: Many AMCs operate hybrid technology environments with some systems remaining on-premises while others have migrated to cloud platforms. Securing these hybrid environments requires managing complex security boundaries.

Emerging Best Practices:

AMCs have developed several effective approaches:

- **Data-centric Security Models**: Leading AMCs have implemented security architectures focused primarily on data protection rather than traditional perimeter defense. These models emphasize data classification, encryption, access controls, and activity monitoring regardless of where data resides.
- **Partner Security Assessments**: Successful AMCs have established structured programs for assessing and enhancing the security posture of distribution partners and service providers. These typically include initial assessment, contractual security requirements, ongoing monitoring, and periodic reassessment.
- **Insider Risk Programs**: Advanced AMCs have implemented dedicated insider risk programs that combine technical controls with human resources processes. These programs typically include separation of duties, privileged access monitoring, behavioral analytics, and structured investigation processes.
- **Cloud Security Frameworks**: To address hybrid infrastructure challenges, many AMCs have developed cloud security frameworks that establish consistent security controls across environments. These frameworks typically establish security responsibilities, configuration standards, and monitoring requirements for each deployment model.
- The establishment of the Asset Management Security Council in 2024 has created a forum for security collaboration across the sector, including joint threat intelligence sharing and collaborative security assessments of common service providers.

Cross-Sectoral Best Practices

Several best practices have emerged across sectors:

- **Risk-based Implementation**: Organizations that align security investments with their specific risk profile typically achieve more effective outcomes than those applying a uniform control set. Successful implementations begin with thorough risk assessment and prioritize controls addressing the most significant risks.
- **Governance Integration**: Effective implementations integrate cybersecurity governance into existing corporate governance structures rather than treating security as a purely technical function. Organizations

with board-level security committees typically demonstrate stronger security cultures and more consistent security funding.

- **Defense-in-depth Architectures**: Leading organizations implement multiple security layers rather than relying on single control points. This approach combines preventive, detective, and responsive controls to create resilience against control failures.
- **Tabletop Exercises**: Regular scenario-based exercises have proven particularly valuable in developing organizational response capabilities. Organizations conducting quarterly executive-level security simulations report significantly improved handling of actual incidents.
- **Automated Compliance Validation**: Organizations that implement automated compliance monitoring typically identify control gaps more quickly than those relying on periodic manual assessments. Continuous compliance validation is emerging as a best practice across the securities sector.
- The implementation of SEBI's cybersecurity framework continues to evolve, with organizations at different maturity levels working to enhance their security posture. While compliance challenges remain, the framework has driven substantial security improvements across India's securities markets, contributing to increased cyber resilience for this critical sector.

5

Technologies Enabling Compliance & Security

5.1 Data Protection & Privacy Tech

The regulatory requirements established by the DPDPA and sectoral frameworks have accelerated adoption of specialized data protection technologies across Indian organizations. These solutions address various aspects of data security, from discovery and classification to encryption and masking.

Data Discovery and Classification

- Effective data protection begins with comprehensive visibility into data assets. Several technology categories have gained prominence in this space:
- Automated Data Discovery Tools: Solutions that scan networks, databases, and storage repositories to identify personal and sensitive data have seen widespread adoption. These tools typically use

pattern matching, machine learning, and content analysis to locate regulated data types. Products including Spirion Data Discovery, ManageEngine DataSecurity Plus, and homegrown solution Kogence DeepScan have gained significant market share in India.

Implementation experience reveals several key considerations:

- Coverage across structured and unstructured data sources is essential for comprehensive discovery
- Performance impact on production systems must be carefully managed through scheduling and throttling
- Classification accuracy requires ongoing tuning with India-specific data patterns (Aadhaar numbers, PAN details, etc.)
- **Data Flow Mapping Tools**: Technologies that track data movement between systems have become increasingly important for addressing DPDPA requirements around purpose limitation and cross-border transfers. These tools monitor data flows through API calls, file transfers, and database connections.
- Leading organizations have implemented continuous data flow monitoring rather than point-in-time mapping exercises. This approach provides ongoing visibility into changing data movements and enables rapid detection of unauthorized flows.
- **Data Classification Frameworks**: Automated classification has been complemented by policy-driven classification frameworks that establish consistent data categories across organizations. Many organizations have aligned classification schemes with regulatory categories (personal data, sensitive personal data, critical personal data) to simplify compliance mapping.

Data Protection Technologies

Once data is discovered and classified, various technologies are employed to protect it:

- **Encryption Solution**s: Encryption adoption has accelerated dramatically, with organizations implementing multiple encryption layers:
- **Transport Layer Encryption**: Nearly universal TLS implementation for data in transit
- **Storage Encryption**: Widespread adoption of transparent database encryption and storage-level encryption

- **Application-Level Encryption**: Growing implementation of field-level encryption for particularly sensitive data elements
- **End-to-End Encryption**: Emerging in specific use cases, particularly secure communications and file sharing
- Indian organizations have faced unique challenges implementing encryption, particularly around key management in complex environments. Many have adopted specialized encryption key management systems that provide centralized policy enforcement and auditability.
- **Tokenization**: For scenarios where data must remain functionally usable while reducing security risk, tokenization has gained traction. This technique replaces sensitive values with non-sensitive tokens while maintaining format and usability. Financial services organizations have been particularly active adopters for protecting payment data.
- Gartner estimates that tokenization adoption in India grew by 35% in 2024, driven by both DPDPA compliance requirements and sector-specific regulations like the RBI's tokenization mandate for card transactions.
- **Data Masking**: Dynamic and static data masking solutions have been widely adopted to protect production data used in non-production environments. These technologies obscure sensitive elements while maintaining referential integrity and functional usability for development and testing purposes.

- Organizations have implemented increasingly sophisticated policies that vary masking approaches based on user role and access context. This "dynamic data masking" approach provides appropriate data access while minimizing unnecessary exposure of sensitive information.

Privacy-Enhancing Technologies (PETs)

- Beyond traditional data protection, advanced privacy-enhancing technologies have begun to emerge:
- **Differential Privacy**: This approach adds carefully calibrated noise to data outputs to prevent individual identification while maintaining aggregate analytical validity. Early adoption has occurred primarily in research contexts and advanced analytics environments, with companies including Tata Consultancy Services, Microsoft India, and Google India implementing differential privacy in specific analytics use cases.
- **Homomorphic Encryption**: This technology allows computation on encrypted data without decrypting it. Though still computationally intensive for many production workloads, partial homomorphic encryption has found applications in specific high-sensitivity scenarios, particularly in financial services and healthcare.
- **Synthetic Data Generatio**n: This technique creates artificial data that maintains statistical properties of original datasets without containing actual personal information. Adoption has grown particularly for AI training and testing scenarios where personal data use would create privacy risks. Indian startups including Synthetic AI and DataMorphix have emerged to address this market.
- **Federated Learning**: This approach trains machine learning models across multiple devices or servers without exchanging the underlying data. Several healthcare initiatives have implemented federated learning to enable research across hospital datasets without centralizing sensitive patient information.

Consent and Rights Management

Managing consent and data subject rights has driven adoption of specialized technological solutions:

- **Consent Management Platforms**: These systems collect, store, and manage user consent preferences across digital touchpoints. Adoption has grown significantly

Consent Management Platforms: These systems collect, store, and manage user consent preferences across digital touchpoints. Adoption has grown

significantly since the DPDPA implementation began, with organizations implementing both commercial platforms and custom-built solutions. Key functionalities typically include:

- Customizable consent collection interfaces
- Centralized consent repositories with comprehensive audit trails
- Preference management capabilities allowing users to modify consent choices
- Integration with marketing and analytics tools to enforce consent choices

Leading vendors in the Indian market include OneTrust, TrustArc, and domestic players like Tsaaro and Privado.io. Implementation experience has highlighted the importance of balancing compliance requirements with user experience considerations. Organizations report that overly complex consent interfaces can increase abandonment rates by 10-15% on digital properties.

Privacy Rights Management Tools: To handle data subject rights requests (access, correction, erasure, etc.), organizations have deployed specialized workflow systems. These tools typically include:

- Web portals for submitting rights requests
- Identity verification mechanisms
- Automated workflows for request processing
- Integration with backend systems to execute requests
- Comprehensive documentation and audit trails

Organizations processing high request volumes report that automation has reduced processing time by 60-80% compared to manual approaches. However, integration challenges with legacy systems remain a significant obstacle, particularly for complex operations like complete data erasure.

Data Subject Request Analytics: As request volumes have grown, organizations have implemented analytics capabilities to understand patterns and optimize response processes. These analytics examine metrics including request types, processing times, and requester demographics. Leading organizations use these insights to identify potential privacy concerns and improve data handling practices proactively.

Emerging Technology Trends

Several emerging technologies are gaining traction to address evolving data protection challenges:

Privacy-as-Code Tools: These solutions integrate privacy requirements directly into development workflows, enabling automated compliance verification during the software development lifecycle. Tools like PrivacyOps and Microsoft's Azure Purview are gaining adoption among technology-focused organizations implementing privacy-by-design approaches.

AI-powered Data Protection: Machine learning techniques are increasingly applied to data protection challenges, including:

- Enhanced personal data detection using natural language processing
- Anomalous access pattern detection for data leak prevention
- Automated privacy impact assessments
- Intelligent redaction of sensitive information in documents

While promising, organizations report that these AI-based solutions still require significant tuning for Indian-specific data patterns and regulatory requirements.

Zero-Knowledge Proof Systems: This cryptographic technique allows one party to prove possession of information without revealing the information itself. Early applications have emerged in identity verification scenarios where organizations can confirm user attributes without accessing underlying identity documents.

India-specific Privacy Technology Adaptations

Several technology adaptations address uniquely Indian requirements:

Aadhaar Data Protection: Specialized solutions have emerged for securing Aadhaar data, implementing the UIDAI's security guidelines. These include masking tools that display only the last four digits and specialized encryption approaches for Aadhaar numbers.

Vernacular Consent Management: Organizations serving diverse linguistic populations have implemented multilingual consent systems supporting all 22 scheduled languages. These solutions incorporate culturally appropriate explanations of data practices rather than direct translations of English text.

Implementation Challenges

Despite technological advances, organizations report several consistent implementation challenges:

Legacy System Integration: Many core business systems were designed before modern privacy requirements. Retrofitting privacy capabilities often requires complex integration work or complete system replacement.

Data Silos: Organizations typically store personal data across multiple disconnected systems, complicating comprehensive discovery and rights fulfillment. Data integration platforms are increasingly deployed to create unified views of customer data across repositories.

Performance Impact: Comprehensive encryption and data scanning can impact system performance. Organizations have developed staged implementation approaches that balance security and operational needs.

As the regulatory landscape continues to evolve, privacy technology adoption is expected to accelerate further. The NASSCOM-DSCI Privacy Tech Market Study projects that India's privacy technology market will grow at a CAGR of 27% through 2027, reaching approximately ₹12,000 crore ($1.5 billion) in annual spending.

5.2 Identity & Access Management (IAM)

Identity and Access Management technologies have become central to implementing regulatory requirements related to data access control, authentication, and authorization. The DPDPA's security safeguard provisions and SEBI's detailed access control requirements have driven substantial IAM investments across regulated entities.

Core IAM Components

Organizations have implemented increasingly sophisticated IAM architectures with several key components:

Authentication Systems: Multi-factor authentication (MFA) has become nearly ubiquitous for access to systems containing regulated data. Implementation approaches include:

- Mobile push notifications (most widely adopted due to user acceptance)

- Hardware security keys (for high-sensitivity roles and critical infrastructure)
- Biometric authentication (growing adoption, particularly in financial services)
- Time-based one-time passwords (common as a backup method)

Leading organizations have implemented risk-based authentication that varies requirements based on contextual factors including device, location, and access patterns. This approach balances security and usability by applying stronger controls in higher-risk scenarios.

Identity Governance Solutions: These platforms manage the lifecycle of identities and their associated access rights. Core capabilities include:

- Automated provisioning and de-provisioning based on HR events
- Access certification workflows for periodic entitlement reviews
- Segregation of duties enforcement to prevent toxic access combinations
- Comprehensive access auditing and reporting

Financial institutions report that formal identity governance implementations have reduced inappropriate access by 30-40% through systematic certification processes. However, implementation complexity remains high, particularly for organizations with diverse and siloed technology environments.

Privileged Access Management (PAM): Solutions specifically focused on controlling, monitoring, and securing privileged accounts have seen significant adoption. These systems typically provide:

- Credential vaulting for administrative accounts
- Just-in-time privilege elevation
- Session recording and monitoring
- Approval workflows for sensitive operations

PAM implementation has accelerated particularly in BFSI sector firms subject to SEBI's enhanced privileged access requirements. Organizations report that these solutions have substantially reduced the risk surface from administrative credentials, though integration with legacy systems remains challenging.

Access Management Platforms: These solutions provide policy-based authorization services across applications and systems. Key capabilities include:

- Centralized policy definition and enforcement
- Fine-grained access control based on multiple attributes
- Dynamic policy evaluation based on contextual factors
- Consistent access control across on-premises and cloud resources

Zero Trust Implementation

The concept of Zero Trust Architecture (ZTA) has gained significant traction, moving from theoretical discussion to practical implementation. This approach assumes no implicit trust based on network location and instead verifies every access request regardless of origin.

Key zero trust implementation patterns include:

Micro-segmentation: Organizations have implemented network segmentation at a much more granular level, with control points between individual application components. This approach limits lateral movement potential in case of compromise but requires sophisticated policy management tools to remain operational.

Identity-aware Proxies: These solutions provide access control at the application level rather than the network level, validating user identity and

context for each request. Deployment often begins with internet-facing applications before extending to internal resources.

Continuous Authentication: Beyond point-in-time login decisions, organizations are implementing systems that continuously evaluate user behavior for anomalies. These solutions can trigger stepped-up authentication or session termination when suspicious patterns appear.

Device Trust Evaluation: Zero trust implementations increasingly incorporate device health and compliance status into access decisions. Organizations have deployed endpoint management solutions that assess device security posture before permitting access to sensitive resources.

While full zero trust implementation remains aspirational for many organizations, phased approaches have proven successful. Financial institutions typically begin with their most sensitive applications before expanding coverage based on risk prioritization.

IAM for Cloud Environments

As cloud adoption accelerates, specialized IAM approaches for cloud environments have emerged:

Cloud Identity Federation: Organizations have implemented identity federation between on-premises directories and cloud services, enabling single sign-on while maintaining central identity governance. This approach supports hybrid operations while reducing the security risks of multiple credential sets.

Cloud Privilege Management: To address the complex permission models of cloud platforms, organizations have deployed specialized cloud security posture management (CSPM) tools. These solutions monitor cloud entitlements, identify excessive permissions, and enforce least-privilege principles across cloud resources.

Cloud Infrastructure Entitlement Management (CIEM): This emerging technology category provides visibility and governance across multi-cloud environments, addressing the unique challenges of managing access across different cloud platforms with inconsistent permission models.

IAM Challenges and Adaptations

Several significant challenges have emerged in IAM implementations:

Identity Fragmentation: Despite federation efforts, most organizations maintain multiple identity repositories. Advanced implementations have deployed meta-directory solutions that create a unified identity view across systems while respecting source system boundaries.

Shadow IT Access: Cloud applications adopted without formal IT approval often operate outside established IAM frameworks. Organizations have implemented cloud access security brokers (CASBs) that discover shadow IT usage and extend access governance to these applications.

Developer Access Management: Securing access in DevOps environments presents unique challenges, as traditional human-centric IAM processes conflict with automation requirements. Organizations have implemented specialized approaches including just-in-time access provisioning, short-lived credentials, and automated secret management.

Contractor and Partner Access: Managing external identities presents particular challenges, especially given DPDPA requirements for vendor oversight. Leading implementations have established dedicated external identity management systems with enhanced verification and monitoring capabilities.

As IAM technologies continue to evolve, integration across security domains has become increasingly important. Advanced implementations now connect identity signals with threat detection systems, creating context-aware security responses that incorporate identity risk into overall security posture assessment.

5.3 Threat Detection & Response

The cybersecurity regulatory landscape has driven significant investments in technologies that detect and respond to security threats. Both the DPDPA's breach notification requirements and SEBI's detailed security monitoring provisions have accelerated adoption of advanced detection and response capabilities.

Security Monitoring Infrastructure

Organizations have implemented increasingly sophisticated monitoring infrastructures:

Security Information and Event Management (SIEM): These platforms aggregate and correlate security data from multiple sources to identify potential threats. Recent implementations have evolved beyond simple log collection to incorporate advanced analytics:

- Machine learning-based anomaly detection
- User and entity behavior analytics (UEBA)
- Automated correlation across multiple data sources
- Risk-based alerting to reduce false positives

While large enterprises typically deploy commercial SIEM solutions from vendors like IBM, Splunk, and Microsoft, smaller organizations increasingly utilize managed SIEM services from providers including Tata Communications, Wipro, and local specialist SecureLayer7.

Network Detection and Response (NDR): These solutions monitor network traffic for malicious activity using a combination of signature-based detection, behavioral analysis, and machine learning. Key capabilities include:

- Encrypted traffic analysis without decryption
- East-west traffic monitoring for lateral movement detection
- Network protocol analysis for application-level threats

- Network topology mapping and device discovery

Financial institutions report that NDR solutions have been particularly valuable for detecting advanced threats that evade traditional perimeter defenses. Leading organizations have implemented NDR across both on-premises networks and cloud environments to maintain consistent visibility.

Endpoint Detection and Response (EDR): This technology category has seen particularly rapid adoption, with solutions deployed on endpoints to detect and contain threats. Modern EDR platforms provide:

- Continuous monitoring of endpoint activity
- Behavioral analysis to identify suspicious patterns
- Automated containment of compromised systems
- Detailed forensic data collection
- Response automation for common threats

The transition from traditional antivirus to EDR represents one of the most significant security technology shifts in recent years. Organizations report substantially improved detection rates for advanced threats, though initial deployment complexity remains challenging for resource-constrained security teams.

Advanced Threat Detection Approaches

Several specialized detection technologies have gained traction:

Deception Technology: This approach deploys decoys and traps to detect attacker activity. Indian organizations, particularly in the financial sector, have implemented deception technologies that create realistic-appearing resources specifically designed to attract attackers. These solutions provide high-fidelity alerts with minimal false positives, though they require specialized expertise to deploy effectively.

DNS Monitoring: Recognizing that most malware relies on DNS for command and control communication, organizations have implemented specialized DNS monitoring solutions. These tools analyze domain reputation, identify domain generation algorithms, and detect DNS tunneling attempts. Financial institutions report that DNS monitoring has been particularly effective at identifying compromised systems within their environments.

Email Security Analytics: Given that email remains the primary initial attack vector, advanced email security solutions have evolved beyond traditional filtering to incorporate behavioral analysis and social engineering detection. These solutions examine communication patterns, writing style, and contextual factors to identify sophisticated phishing attempts.

Cloud-Native Security Monitoring: As workloads migrate to cloud environments, organizations have deployed cloud-native security monitoring solutions. These tools analyze cloud provider logs, API calls, and configuration changes to identify security issues. Implementation approaches include cloud security posture management (CSPM) for configuration monitoring and cloud workload protection platforms (CWPP) for runtime threat detection.

Security Orchestration and Automated Response

To address the challenge of alert volume and response speed, organizations have implemented security orchestration, automation, and response (SOAR) platforms. These solutions provide:

- Playbook-based response automation for common scenarios
- Case management for security incidents
- Integration across security tools for coordinated response
- Metrics and reporting on response effectiveness

Indian organizations report that automation has reduced response times for common scenarios by 60-90%, allowing security teams to focus on more complex threats. Implementation typically begins with simple use cases like phishing response before progressing to more sophisticated scenarios.

Advanced implementations have integrated threat intelligence platforms with SOAR solutions, enabling automatic enrichment of security alerts with relevant threat data. This integration helps analysts prioritize alerts based on relevance to the organization's specific threat landscape.

Managed Detection and Response Services

Recognizing the challenges of building in-house security operations capabilities, many organizations have turned to managed detection and response (MDR) providers. This service model combines technology, processes, and security expertise to deliver 24x7 threat monitoring and response.

The Indian MDR market has evolved significantly, with offerings from global providers like Mandiant and CrowdStrike as well as domestic players including Tata Communications, Tech Mahindra, and specialized providers like Securenass. Industry-specific MDR offerings have emerged for sectors with unique regulatory requirements, particularly financial services and healthcare.

Small and medium enterprises have been particularly active MDR adopters, finding that the service model provides more advanced capabilities than they could build internally. Larger organizations often implement hybrid models, using MDR for specific environments or as after-hours augmentation of internal teams.

Incident Response Technologies

To support effective incident handling, organizations have deployed several specialized technologies:

Digital Forensics Platforms: These solutions preserve and analyze evidence from compromised systems. Advanced implementations include memory forensics capabilities and automated evidence collection from cloud environments.

Threat Hunting Platforms: Going beyond alert-driven response, these tools support proactive searching for signs of compromise. They typically provide hypothesis-driven investigation workflows and visualization tools to understand complex attack patterns.

Breach Impact Assessment Tools: To support the DPDPA's breach notification requirements, organizations have implemented technologies that help determine affected data and individuals following a security incident. These solutions analyze compromised systems to identify accessed data and affected data subjects.

Implementation Challenges

Despite significant advances, organizations report several persistent challenges in detection and response implementations:

Alert Fatigue: Even with improved analytics, security teams face overwhelming alert volumes. Leading organizations have implemented risk-based alerting that incorporates asset value, vulnerability status, and threat intelligence to prioritize the most significant alerts.

Visibility Gaps: Modern environments span on-premises systems, multiple cloud providers, and remote endpoints, creating significant visibility challenges. Organizations have implemented centralized logging architectures and unified monitoring platforms to address these gaps, though complete visibility remains elusive for complex environments.

Skilled Personnel Shortages: Advanced detection technologies require specialized skills for effective operation. Organizations have addressed this through a combination of automation, managed services, and innovative staffing models including rotational security roles and university partnerships.

As threats continue to evolve in sophistication, detection and response technologies will remain a critical focus area for regulatory compliance and effective security risk management.

5.4 Compliance & Governance Tools

The complexity of India's cybersecurity regulatory landscape has driven adoption of specialized tools that help organizations manage compliance requirements, demonstrate adherence, and maintain governance oversight. These solutions address the administrative aspects of compliance management while providing necessary documentation for regulatory examinations.

Compliance Management Platforms

Organizations subject to multiple regulatory frameworks have implemented comprehensive compliance management solutions:

Integrated GRC Platforms: Governance, Risk, and Compliance (GRC) platforms provide unified approaches to managing regulatory requirements. Key capabilities include:

- Control mapping across multiple regulatory frameworks
- Control testing and evidence collection workflows
- Compliance status dashboards and reporting
- Issue tracking and remediation management
- Documentation and artifact management

Leading GRC implementations establish common control frameworks mapped to multiple regulations. This approach allows organizations to address overlapping requirements efficiently rather than treating each regulation separately.

Financial services organizations report that integrated GRC platforms have reduced compliance documentation effort by 30-40% by enabling evidence reuse across multiple regulatory requirements. The most effective implementations integrate with security tools to automate evidence collection rather than relying on manual documentation.

Specialized Regulatory Compliance Solutions: Beyond general GRC platforms, specialized solutions focused on specific regulations have gained adoption. For DPDPA compliance, these tools typically include:

- Data process inventory management
- Data protection impact assessment workflows
- Consent tracking and documentation
- Rights request management
- Breach notification tracking

For SEBI requirements, specialized solutions provide capabilities including:

- Cybersecurity control documentation
- Independent assessment management
- Vulnerability remediation tracking
- Security metrics reporting aligned with regulatory expectations

Cloud Compliance Management: As organizations migrate to cloud environments, specialized cloud compliance tools have emerged. These solutions continuously monitor cloud configurations against regulatory requirements, industry frameworks, and organizational policies. Key capabilities include:

- Automated compliance scanning
- Configuration drift detection
- Compliance status visualization
- Automated remediation for common issues

Leading implementations integrate cloud compliance tools with CI/CD pipelines to prevent deployment of non-compliant resources. This “shift-left” approach addresses compliance issues during development rather than after deployment.

5.4. Policy Management Systems

Policy management systems have emerged as critical tools for organizations navigating India’s complex regulatory environment. These platforms streamline the creation, distribution, and enforcement of security policies across organizations, ensuring alignment with regulatory requirements.

Key features of modern policy management systems include:

- Centralized policy repositories
- Automated policy distribution and acknowledgment tracking
- Version control and audit trails
- Integration with training and awareness platforms
- Compliance mapping and gap analysis capabilities
- Real-time policy enforcement monitoring

Leading organizations are implementing these systems to maintain comprehensive policy libraries that can be quickly updated in response to regulatory changes, with automatic notification systems ensuring stakeholders remain informed of policy updates.

6

Startups and Innovation in the Cybersecurity Space

6.1. The Indian Cybersecurity Startup Ecosystem

India's cybersecurity startup ecosystem has experienced remarkable growth, with over 350 active cybersecurity startups as of early 2025. These companies are addressing critical security challenges through innovative technology solutions while creating a robust national security posture.

The ecosystem is characterized by:

- Concentration in key tech hubs: Bangalore, Hyderabad, Pune, and the NCR region
- Growing venture capital interest, with cybersecurity investments reaching new milestones.

- Strong technical talent from premier institutions like IITs, NITs, and IIIT
- Emerging focus on “Made in India” security solutions aligned with the Atmanirbhar Bharat initiative

One of the Key government initiatives supporting the ecosystem include National Centre of Excellence (NCoE) This flagship initiative by MeitY in collaboration with DSCI has significantly enhanced India’s cybersecurity innovation ecosystem:

- Development of indigenous cybersecurity products and intellectual property
- Advanced R&D programs in emerging areas like quantum-safe cryptography
- Specialized labs and testing facilities for security product validation
- Comprehensive startup acceleration programs supporting over 80 ventures
- National-level policy development and implementation support
- Coordination with other centers and initiatives across the country

DSCI - Cybersecurity Centre of Excellence (CCoE), Telangana Supporting the national initiative, this regional center focuses on:

- Startup incubation and acceleration in the Hyderabad ecosystem
- Industry-academia collaboration within the region
- Market access support for early-stage security companies
- Specialized mentorship networks for security entrepreneurs

Additional Support Mechanisms

- The Cyber Security Grand Challenge with prizes worth ₹6.3 crore
- State-level initiatives complementing national programs
- Industry-specific security innovation programs

The collaborative model between government agencies, industry associations, and academic institutions has created a robust foundation for cybersecurity innovation, positioning India as an emerging hub for security technology development while addressing India-specific challenges.

6.2. Select Startups & Their Offerings

Born out of deep-dive forensics on some of India's earliest card-breach investigations, Bengaluru-based SISA has evolved from a PCI-DSS audit boutique into a full-stack cyber-resilience partner. Its flagship ProACT MXDR service couples 24×7 SOC analysts with machine-learning analytics to squash dwell time, while SISA Radar crawls data lakes to surface stray PANs or Aadhaar numbers before attackers do. The company backs its technology with heavy-duty credentials—CREST, CERT-In and PCI SSC listings plus an ANAB-accredited training arm—and today protects more than 2,000 payment-heavy organisations across forty countries.

Hyderabad start-up SecurWeave bets that the surest way to stop kernel-level malware is to make the silicon itself play bouncer. Its CHESS-P micro-hypervisor grafts onto modern CPU virtualisation extensions, ring-fencing the operating-system kernel and OT workloads with near-zero performance drag. The same technology is already flying inside IIT-Madras' open-source Shakti processors and is now being piloted for avionics and drone control where deterministic security trumps patch-and-pray approaches.

Gurugram-based Saptang Labs looks after digital reputations with Sarvagya, a one-stop portal that sweeps the surface web, dark web, rogue APK stores and social channels for brand abuse, credential leaks and fake apps. What clients like most is the "local-first" culture—threat-intel analysts who speak Hindi, Marathi or Tamil can jump on takedowns in hours rather than days, a speed edge that has won the firm a slate of BFSI and fast-fashion e-commerce logos in the past year.

If a surveillance camera, conveyor PLC or smart-meter has a CVE, chances are Redinent found it first. The Bengaluru outfit blends passive fingerprinting with active fuzzing to map and score thousands of IoT devices in real time; its research team has published multiple zero-days, including the 2022 Milesight IP-camera DoS flaw that triggered an industry-wide patch scramble. Nokia recently tapped Redinent for an Industry 4.0 security pilot, underlining its growing clout in cyber-physical risk management.

Kochi-headquartered Prophaze rewired the traditional web-application firewall so it sits natively inside Kubernetes. Drop-in ingress-controller integration means DevOps teams get OWASP-Top-10 and API-abuse coverage with almost no latency tax; the platform auto-scales pods during DDoS spikes and feeds clean traffic back to service meshes like Istio. Recognition in Gartner's 2024 Market Guide for API Protection helped Prophaze land healthcare and gaming giants looking to harden micro-services without slowing CI/CD.

Quantum computers may be a decade away from cracking RSA, but QNu Labs isn't waiting. Its Armos QKD appliance ships photons down standard fibre to deliver information-theoretic key exchange, while Tropos QRNG and Hodos post-quantum crypto SDK round out a "quantum-safe stack" already listed on India's GeM procurement portal. Seven granted patents and pilots with defence agencies have put the Bengaluru firm on the radar of global CIOs drafting quantum-migration roadmaps.

Mumbai's Protectt.ai tackles the exploding mobile-fraud surface. Its AppProtectt SDK injects runtime self-protection straight into Android or iOS builds, spotting emulators, code tampering and screen-scraping in milliseconds; a linked threat-intel cloud feeds real-time risk scores back to bank and wallet apps now installed on 200-plus million devices. Expansion into the GCC via channel partners this year underscores demand for app-centric XDR beyond India.

Start-up	Core Focus	Flagship Products / Services	Stand-out Differentiators
SISA (Bengaluru)	Forensic-driven cyber-defence for payment ecosystems	ProACT MXDR – managed XDR platform SISA Radar – data discovery & classification PCI, GDPR, ISO & SOC compliance services	16 years of payment-forensics DNA; 2,000+ customers in 40+ countries; ANAB-accredited training arm and CREST, CERT-In, PCI-SSC recognitions

Start-up	Core Focus	Flagship Products / Services	Stand-out Differentiators
SecurWeave (Hyderabad)	Hardware-rooted security for critical embedded & OT systems	CHESS-P (Kernel & Application Protector) CHESS-E (Deep Isolator) forthcoming Next-Gen SIEM	Lightweight security hypervisor that taps processor virtualisation extensions to stop zero-day kernel-mode malware; co-engineered with IIT-Madras "Shakti" processors
Saptang Labs (Gurugram)	Brand-centric digital-risk protection	Sarvagya digital-threat-intel suite covering app, dark-web, social-media, credential-leak & bot monitoring	Single console for seven threat streams; 99 % Android app-spoof detection coverage and bespoke takedown playbooks for enterprises
Redinent (Bengaluru)	Cyber-physical & IoT vulnerability intelligence	Cloud-delivered platform blending Deep Asset, Vulnerability & Threat Intelligence Redinent VI (Contextual Risk Prioritisation)	CVE research team credited with multiple zero-day disclosures; selected by Nokia for industrial IoT security pilot; Forbes DGEMS "Select 200" 2024
Prophaze (Kochi)	Cloud-native API & application defence	Kubernetes-native WAF Hybrid/Cloud WAF, Bot & L7 DDoS protection, WAAP	Runs as an ingress controller that auto-scales with clusters; recognised as a "Top API-Security Vendor" in Gartner 2024 Market Guide
QNu Labs (Bengaluru)	Quantum-safe cryptography	Armos QKD Tropos QRNG Hodos PQC QShield™ integrated quantum-security platform	First Indian firm shipping commercial QKD; products listed on GeM & AWS Marketplace; 7 granted patents and White-House-aligned quantum-migration roadmap

Start-up	Core Focus	Flagship Products / Services	Stand-out Differentiators
Protectt.ai (Mumbai)	Mo-bile-threat defence & real-time fraud con-trol	AppProtectt Mobile-App RASP XDR APIProtectt MobileProtectt device-risk engine	Runtime in-app self-protection that now secures > 200 M Indian smartphones; expanding via GCC partnership with Finesse/TechBridge MEA

6.3. Case Studies

Indian cybersecurity startups have demonstrated significant impact across sectors:

Case Study 1 – Banking & Payments (PCI Compliance + XDR)

A leading Indian private-sector bank combined SISA Radar to catalogue 14 million sensitive records with the ProACT MXDR service, cutting false-positive alerts by 40 % and shaving three weeks off its annual PCI-DSS re-certification cycle.

Case Study 2 – Critical Infrastructure / Defence-grade Embedded Systems

During IIT-Madras' "Shakti" RISC-V processor programme, SecurWeave's CHESS-P hypervisor was fused at silicon level, giving drone-control units deterministic isolation and kernel-rootkit resistance. Field tests showed zero successful exploits across 72 hours of red-team emulation against APT-style firmware attacks.

Case Study 3 – Industrial IoT Security in Manufacturing

When an Industry 4.0 assembly line migrated 1,100 CCTV & OT sensors to an IP backbone, Redinent's platform fingerprinted 97 % of white-label cameras correctly, surfaced 43 critical CVEs and generated a patch-plan aligned to ISO 27001/NIST CSF—work later showcased in Nokia's joint industrial-IoT security paper.

Case Study 4 – Mobile-first FinTech Fraud Mitigation

A Tier-1 wallet app that processes 28 M transactions/day embedded Protectt.ai's AppProtectt RASP SDK. Within the first quarter it blocked 1.3 M emulator-driven attacks, reduced account-takeover fraud by 61 %, and provided regulators with machine-readable RBI-DPSC compliance evidence.

Case Study 5 – Cloud-native e-Commerce Defence

A fast-growing D2C platform running on EKS replaced its stock NGINX ingress with Prophaze Kubernetes WAF. The switch delivered sub-5 ms latency overhead while deflecting a 87 Gbps bot-net DDoS burst and meeting OWASP API-Top-10 coverage, letting DevOps keep blue/green deployments fully automated.

7

Emerging Trends & The Road Ahead

Several trends will shape India's cybersecurity regulatory landscape in the coming years:

AI Governance Frameworks The National AI Strategy and upcoming AI regulations will establish guardrails for responsible AI deployment, with specific provisions for AI-based security tools. Organizations must prepare for algorithmic accountability and transparency requirements.

Critical Information Infrastructure Protection Enhanced regulations for critical sectors (energy, finance, healthcare) will emerge, with stricter compliance requirements and potential penalties for non-compliance. Mandatory security assessments and incident reporting will become more rigorous.

Supply Chain Security Regulations New frameworks addressing digital supply chain risks are expected

by late 2025, requiring organizations to implement vendor assessment mechanisms and continuous monitoring capabilities.

Regulatory Technology (RegTech) The convergence of compliance and security technologies will accelerate, with AI-driven solutions automating compliance monitoring and reporting. This will reduce compliance costs while improving effectiveness.

International Harmonization Efforts India is likely to participate more actively in global cybersecurity norm-setting, working toward mutual recognition frameworks while maintaining sovereignty over critical data assets.

Sector-Specific Evolution Financial services regulations will continue to lead in sophistication, with SEBI and RBI frameworks serving as models for other sectors. Healthcare data protection will see significant regulatory development in response to digitization initiatives.

The regulatory landscape will continue to evolve rapidly, requiring organizations to develop adaptive compliance strategies and invest in forward-looking security capabilities.

8

Conclusion

8.1. Key Takeaways

India's cybersecurity regulatory landscape represents a dynamic ecosystem balancing security, privacy, and innovation imperatives. As digital transformation accelerates across sectors, regulatory frameworks will continue to evolve, requiring organizations to adopt proactive compliance strategies.

Key takeaways from this analysis include:

1. **Proactive compliance provides competitive advantag**e: Organizations that view cybersecurity regulations as strategic enablers rather than cost centers gain market advantages through enhanced trust and operational resilience.
2. **Integration is essential**: Successful organizations are integrating security, privacy, and compliance functions rather than treating them as separate domains.
3. **Technology enables compliance**: Emerging tools and platforms are reducing compliance burdens

while improving effectiveness, particularly when implemented as part of a comprehensive security strategy.

4. **Regulatory evolution will continue**: India's regulatory framework will continue to mature, likely incorporating global best practices while addressing unique national priorities.
5. **Innovation ecosystem is expanding**: India's growing cybersecurity startup ecosystem is developing solutions specifically designed for the national regulatory context.

India stands at a critical juncture in its cybersecurity regulatory journey. The establishment of comprehensive frameworks like the DPDPA represents significant progress, yet challenges remain in implementation and harmonization across sectors.

The path forward requires collaboration between government agencies, industry stakeholders, technology providers, and security professionals. By fostering this collaborative ecosystem, India can develop regulatory frameworks that enhance digital trust while enabling innovation.

As organizations navigate this complex landscape, those that embrace security and compliance as strategic imperatives rather than regulatory burdens will be best positioned to thrive in India's digital economy. The coming years will likely see further evolution in this space, requiring continued vigilance and adaptation from all stakeholders.

9 Appendices

9.1. Glossary of Terms

CERT-In	:	Computer Emergency Response Team - India
DPDPA	:	Digital Personal Data Protection Act
DPI	:	Digital Public Infrastructure
DSCI	:	Data Security Council of India
FRB	:	Future Ready Businesses
IAM	:	Identity and Access Management
MeitY	:	Ministry of Electronics and Information Technology
NCIIPC	:	National Critical Information Infrastructure Protection Centre
NPCI	:	National Payments Corporation of India
PDP	:	Personal Data Protection
RBI	:	Reserve Bank of India
SEBI	:	Securities and Exchange Board of India
SPDI	:	Sensitive Personal Data and Information
VAPT	:	Vulnerability Assessment and Penetration Testing

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

The National Centre of Excellence (NCoE) for Cybersecurity Technology Development has been conceptualized by the Ministry of Electronics & Information Technology (MeitY), Government of India, in collaboration with the Data Security Council of India (DSCI). Its primary objective is to catalyze and accelerate cybersecurity technology development and entrepreneurship within the country. NCoE plays a crucial role in scaling and advancing the cybersecurity ecosystem, with a focus on critical and emerging areas of security.

Equipped with state-of-the-art facilities, including advanced lab infrastructure and test beds, NCoE enables research, technology development, and solution validation for adoption across government and industrial sectors. By adopting a concerted strategy, NCoE aims to translate innovations and research into market-ready, deployable solutions—contributing to the evolution of an integrated technology stack comprising cutting-edge, homegrown security products and solutions.

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

DATA SECURITY COUNCIL OF INDIA

+91-120-4990253 | ncoe@dsci.in

https://www.n-coe.in/

4 Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303

Follow us on

@CoeNational
nationalcoe
nationalcoe
NationalCoE