RBI Advisory on Customer Data Protection and Management

Published by Reserve Bank of India (RBI), Department of Supervision, Central Office Cyber Security and IT Risk (CSITE) Group

Financial Services

—

April 2026

KPMG. Make the Difference.

Table of Contents

Introduction

Introduction to the Advisory

RBI CSITE Group conducted a thematic study on “Security of customer data” across Supervised Entities (SEs) covering multiple categories of supervised entities in 2025, to identify several best practices that are being followed for protection of customer data in the SEs’ ecosystem and published an advisory to summarise the same as guidance for SEs in strengthening their framework for protection of customer data

Applicability

- Public sector banks
- Private sector banks
- Foreign banks
- Small finance banks
- Payment banks
- Non-banking financial companies
- All India financial institutions

Key stakeholders impacted

- **Board of Directors**
- **Steering Committee**
- **Senior Management**
- **Security operations center (SOC) Team**

Objective

- SEs must prioritise robust customer data protection framework
- Establish and continuously enhance cyber security and data-protection mechanisms to safeguard customer information across the entire digital ecosystem
- Adherence to all applicable laws, regulations, and supervisory guidelines related to data protection

Leading practices

- Establishing a clear governance structure to protect customer data properly, ensure accuracy and regulatory compliance, the process for data collection, classification, and data use needs to be defined
- Protection of customer data during accessing from anywhere, sharing and third-party interactions requires the implementation of strong security controls with structured approach of cloud security to manage risks to customer data on cloud platforms as well
- Defined data retention and destruction processes to avoid keeping customer data longer than necessary and to minimize security risks
- Robust framework for tracking complaints and grievance redressal is necessary to empower customers and ensure transparency
- Defined framework is required for incident response, simulation exercises, and customer communication, with layered security controls and 24x7 monitoring to enable continuous detection, alerting, and response to threats involving customer data
- Security of customer data requires defined measures for its discovery, classification, encryption, and monitoring.

Overview of the CSITE advisory

Domain overview (1/2)

Domains	Advisory Requirements
1 Governance and regulatory compliance	• Enforce *board-level approval* and periodic review pertaining to customer data security, privacy, and third-party risk policies • *Formally assign roles* for customer data protection and mandate periodic reporting to senior management and the board • Establish responsible accountable consulted informed (*RACI*) matrix-based accountability structure to define and document responsibilities across functions and put in place a cross-functional steering committee to oversee customer data governance and related risks.
2 Data collection, classification, and usage	• Adopt *automated tools* to identify, label and manage customer data for consistent tagging and classification. This is executed on predefined sensitivity levels, across on-prem, cloud, and third-party environments • Employ a *unified platform* that captures, tracks, and updates customer consent consistently, and in an auditable manner • *Clearly convey* data collection, usage purposes, and customer rights at key interaction points.
3 Data inventory and data security controls	• Execute *periodic and detailed data discovery* exercises enabling the identification, inventory, classification and mapping of customer data across different systems. Put in place strong cryptographic standards along with Hardware Security Models (HSMs) • Monitor all endpoints using *multi-layered data leakage prevention* to identify and block unauthorised data leakage • *Standardisation of naming and classification*, thereby improving the consistency in identification and protection of customer data.
4 Data access management	• Implement encrypted Virtual Private Network (VPN), Virtual Desktop Infrastructure (VDI) restrictions, SOC monitoring, and endpoint protections like Endpoint Detection And Response (EDR) and Data Leakage And Prevention • Use Mobile Device Management (MDM) for device encryption, secure containers, remote wipe, and restrictions on copy-paste and screenshots • Keep in place *comprehensive access logs*, incorporated with Security Incident And Event Management (SIEM) / Database Access Management (DAM), and provide real-time alerts for unauthorised or unusual activity.
5 Data sharing and Third-party Risk Management	• Provide *only necessary customer data* with clearly defined scope, arrangements, and required safeguards • Carry out *detailed due diligence for third party vendors* prior to onboarding and periodic assessments of accesses post onboarding • Make certain prompt reporting of customer data breaches by third party vendors and prohibit storage of sensitive customer data as plain text.
6 Continuous monitoring / real time oversight	• Apply multi-layered tool such as SIEM, DAM, DLP and EDR for consistent detection and response to suspicious activities related to customer data • Install 24x7 monitoring through SOC and combine solution logs, DAM and DLP with SIEM systems for real-time reviewing on customer data management and threat response to secure customer data.

Domain overview (2/2)

Domains	Advisory Requirements
7 Incident response and recovery	• Incident response framework recording any scenario related to *customer data guarantees prompt detection and escalation* with severity identification • Carry out *cyber drills*, addressing various scenarios and onboarding third party for identification of blind spots, testing cyber resilience and optimising coordination under stress • Assure *clear customer notification* through various channels and remediation guidance. Documentation of these practices in the Cyber Crisis Management Plan (CCMP) confirming consistency and customer- first approach.
8 Data retention and destruction	• Document the *duration of retention and deletion* as per legal, regulatory and organisational requirements for *customer and non-customer data* • Conduct through periodic reviews adherence to defined durations and document audit trails containing authorised, traceable and verifiable logs • Put into effect standardized destruction methods as defined by *NIST 800-88* or equivalent.
9 Customer rights and empowerment	• Deployment of Customer Relationship Management (CRM) for the generation of *unique customer complaint reference numbers* and automatic notification on complaint registration in cases of customer data misuse • Provide a framework encompassing multiple channels for grievance redressal, hierarchy for escalation matrix, communication protocols and turnaround times.
10 Audit and testing	• Incorporate customer data security in internal/ IS audit scope along with results of Vulnerability Assessment And Penetration Testing (VAPT) • Inclusion of, as applicable, *third-party cybersecurity and customer data protection measures* for the usage of customer data by third parties • Requirement to maintain extensive audit logs of all customer data modifications, storage encryption, role-based access controls, log retention, periodic reviews and forensic readiness.
11 Emerging technologies and data risks	• Reduction of data exposure through Application Programming Interface (API) gateway enforcement, secured hosting of data during usage of chatbots and Artificial Intelligence (AI) solutions • Establish applicable governance, monitoring and risk mitigation mechanisms for utilisation of AI/ Machine Learning (ML) or equivalent technologies • Put into effect SIEM platforms, API monitoring in real- time, detection of anomalies, performance evaluation and penetration testing at regular interval for efficient identification and mitigation of security risk.
12 Data security in external systems (cloud)	• Define cloud security based baselines for domain hosting customer data, Identity and Access Management (IAM), network controls, encryption, logging, backup and key management comparable to the on-site environment • Utilize *Cloud Security Posture Management* (CSPM) and built in cloud tools to maintain up to date records of cloud assets and data stores, monitor for public access and consistently report critical issues to the senior management • Maintain clear *insights and documentation of the security duties shared* between the cloud service provider for systems handling customer data.

Key imperatives for SEs

Key imperatives for SEs

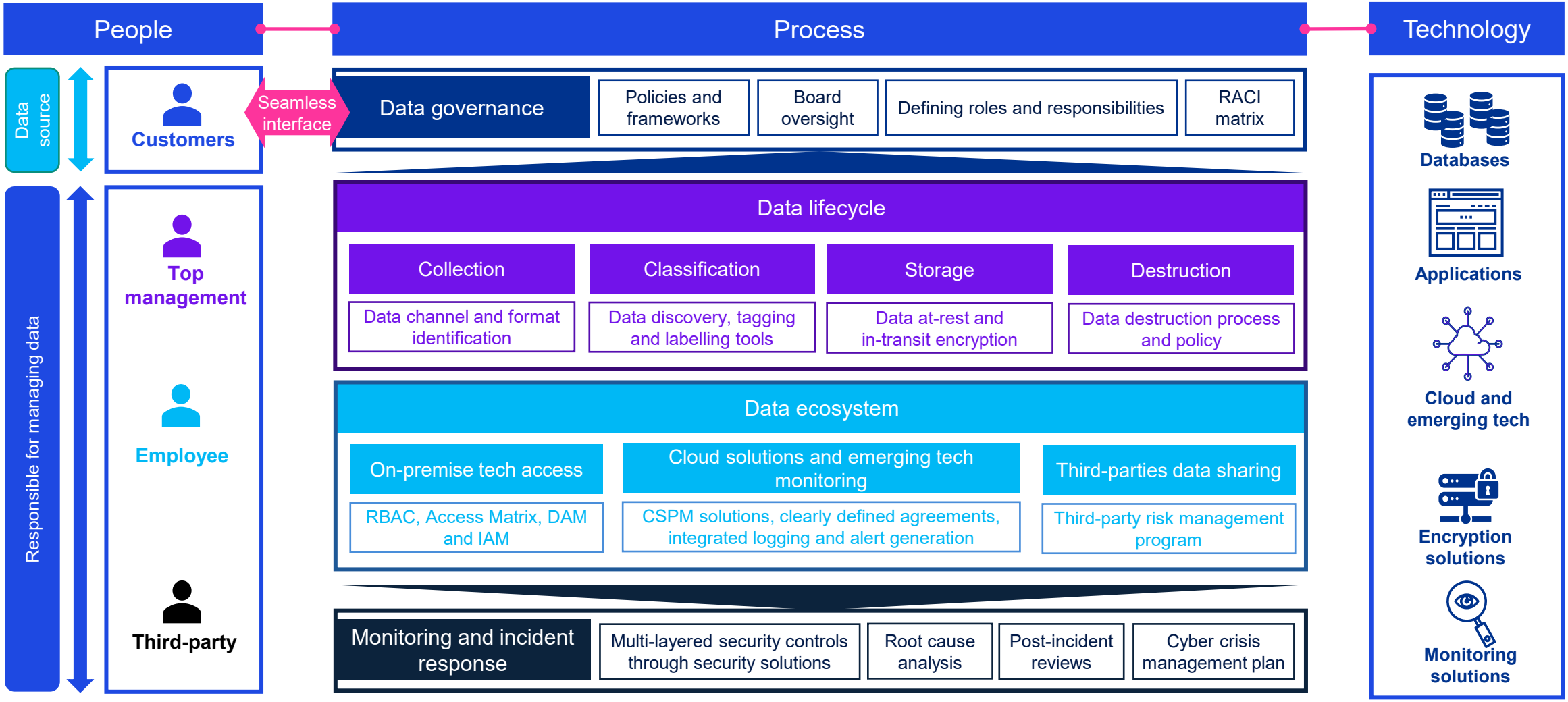
	Challenges	Approach	Outcome
1	**Data Governance and Classification** Limited visibility of data across SE's ecosystem due to fragmented data identification, classification, and metadata practices	• Establish an enterprise-wide data discovery, classification, and metadata management framework across the data lifecycle	Consistent visibility of customer data flows and strengthened enterprise data governance
2	**Data Security – Encryption, Key Management** Growing volumes of sensitive customer data increase the complexity of securing data while enabling legitimate business use	• Implement standardised encryption and centralised key management aligned to data sensitivity and usage	Enhanced protection of customer data with secure enablement of business processes
3	**Identity and Access Management** Inconsistent access controls elevate the risk of unauthorised or inappropriate access to data	• Strengthen access governance through IAM solutions with RBAC, access matrices, DAM, and endpoint security controls	Controlled, role-based access to customer data and reduced access-related risks
4	**Monitoring and Threat Detection** Limited oversight of data activity across the tech-landscape constrains timely detection of security events	• Deploy centralised monitoring by integrating SIEM, DLP, DAM, UEBA, and SOC-based oversight	Timely detection, investigation, and containment of customer data security incidents
5	**Incident Response and Recovery** Absence of a structured and tested incident response capability may delay containment and recovery from data-related incidents	• Establish a formal Incident Response and Recovery framework with RCA, cyber drills, and crisis communication protocols	Improved incident responsiveness, effective recovery, and transparent customer communication

Key imperatives for SEs

Challenges	Approach	Outcome
6 **Data Retention and Destruction** — Inconsistent data retention and destruction practices increase the risk of unnecessary data exposure and regulatory non-compliance	• Define retention schedules, enforce audit trails, and implement secure data destruction mechanisms 	Reduced data over-retention risks and improved compliance with retention requirements
7 **Regulatory Compliance and Governance** — Heightened regulatory expectations require continuous alignment across policies, processes, and technical controls	• Implement centrally governed compliance frameworks, policy reviews, and approval mechanisms 	Sustained regulatory alignment with clear accountability and governance oversight
8 **Third-Party and Cloud Risk Management** — Limited oversight of third-party and cloud-hosted customer data increases governance and security risks	• Strengthen third-party assessments and enforce cloud security baselines with CSPM-based monitoring 	Consistent security posture and improved oversight across vendors and cloud environments
9 **Emerging Technology Risk Management** — Adoption of APIs, AI, and emerging technologies introduces incremental data exposure risks if not governed appropriately	• Enforce secure API management, AI governance frameworks, and continuous risk monitoring 	Controlled and secure adoption of emerging technologies involving customer data
10 **Customer Communication** — Inconsistent methods of tracking progress though the complaint lifecycle which lead to confusion and reduced transparency for customers	• Automated process for communicating a unique Complaint Reference Number when a complaint is lodged and also when it is closed 	Consistent and transparent complaint tracking

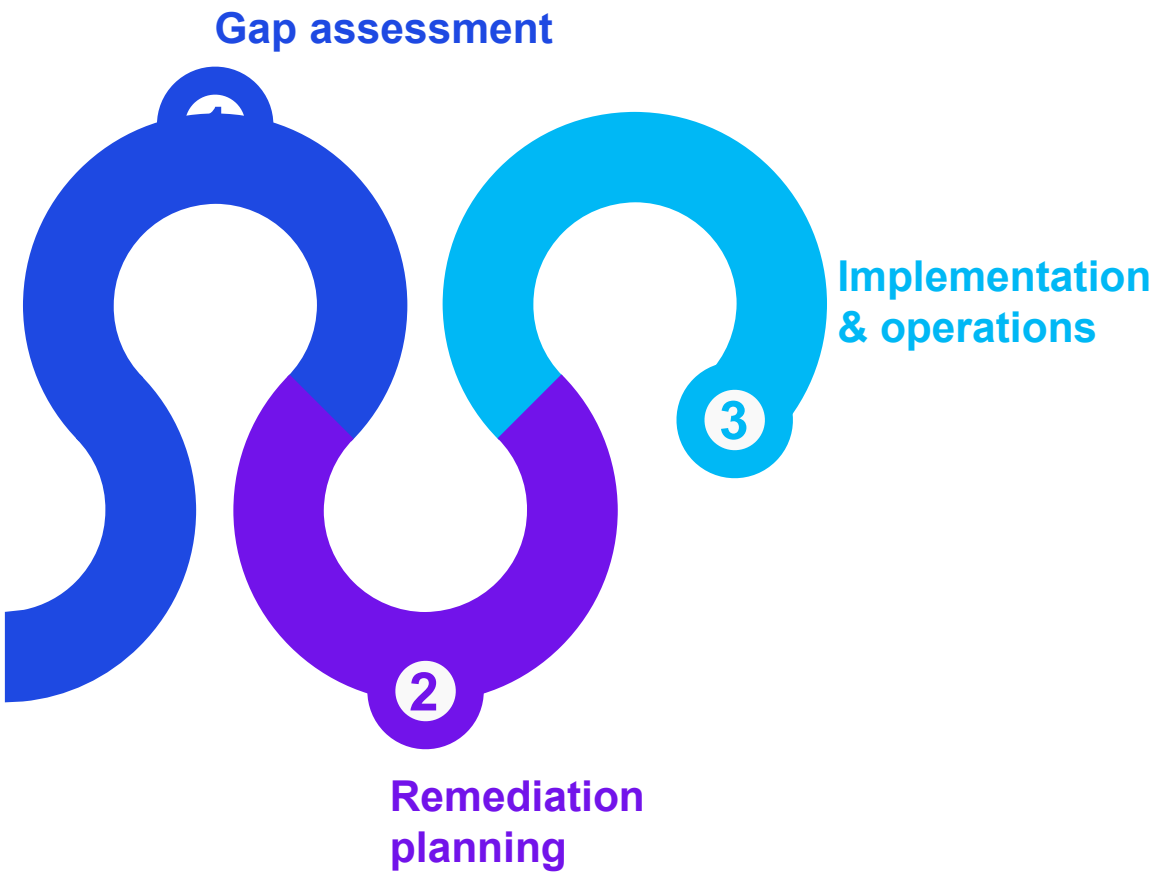
Proposed data landscape at SEs

Leveraging our vast experience across financial sector, KPMG in India has prepared the below proposed data-landscape at SEs in a structured format mapped across People, Process and Technology aligned with this advisory



Way forward

How KPMG in India can help



Gap assessment

- Conduct a gap assessment of the existing data protection framework and data lifecycle
- Assess current SOC monitoring tools and controls for possible data leaks
- Review existing data discovery, classification and DLP capabilities for critical systems

Remediation planning

- Devise a priority-based and risk-based issue remediation plan
- Define enhancements for data protection controls and finding opportunities for streamlining usage of technology

Implementation & operations

- Phase wise gap closure implementation
- Focus on re-configuration and optimisation of existing security tools and monitoring capabilities
- Supporting with project management and running operations on behalf of SEs
- Use continuous monitoring to safeguard compliance and protection

Why KPMG in India ?

Regulatory alignment
Helping clients achieve regulatory alignment by bridging gap between data protection norms defined by the regulators and data governance frameworks tailored for their environment

Strengthening cybersecurity and risk management
Assisting in fraud risk mitigation and secure encryption protocols to data integrity

Data lifecycle management and retention controls
Helping organisations manage data ensuring information is retained as long as it is necessary and destroyed post retention period

Financial sector focus
Engaged with key players in India's financial services ecosystem including banks, third party application providers, and aggregators

Streamlining data management
Assisting in review of regulatory submissions for financial institutions

Below are KPMG in India's select credentials in the data protection space-

Multinational bank	Insurance companies	Large Indian bank	Global card payment network
Global payment aggregators	Payment gateways	Indian private sector bank	Indian PSUs

Acknowledgements

Contributors:

- Aakansha Gupta
- Madhuri Gangaramani
- Shubham Sharma
- Aayush Gandhi
- Siddhi Jani

Source: Advisory on Best Practices for Customer Data Protection, March 2026, RBI – Department of Supervision, Central Office Cyber Security and IT Risk Group

KPMG in India contacts :

Akhilesh Tuteja
Global Head
Cyber Security
E: atuteja@kpmg.com

Atul Gupta
Partner, Head of Function
Digital Trust and Cyber
E: atulgupta@kpmg.com

Kunal Pande
Partner, Leader - Digital Trust & Cyber for
FS, Co-Head - Digital Risk & Cyber
E: kpande@kpmg.com

Rohan Padhi
Partner and Co-Lead
Digital Risk and Cloud Security
E: rohanpadhi@kpmg.com

Romharsh Razdan
Partner, Lead Payment Risk and
Co-Lead Cloud Security
E: romharsh@kpmg.com

kpmg.com/in

Access our latest insights on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.