Enhancing Banking Security and Compliance: Navigating RBI Guidelines with a Data-Centric Approach

The Two Towers – Security and Compliance

Banking executives are increasingly concerned about how outsourcing affects compliance and security. According to the Reserve Bank of India (RBI) guidelines, banks must disclose all outsourced IT services in their outsourcing policies. The guidelines also outline specific responsibilities for the bank's board and senior management, including clear expectations for decision-making processes, risk management, and compliance. Additionally, it includes detailed regulations for individuals who hold simultaneous roles on the board and in senior management positions, covering areas such as conflicts of interest and ethical standards.

Indian banks face significant security and compliance challenges. While organizational complexity may seem straightforward, it often becomes paradoxical in practice. For example, banks and their service providers (like printing and calling vendors) must delete confidential information when it's no longer needed. Contracts often mandate that confidential information and related assets be destroyed when a business relationship ends. However, relying solely on paper contracts or NDAs is insufficient to ensure and validate that this information has been destroyed in compliance with RBI Guidelines. A proactive data-centric approach is essential for banks to meet regulatory requirements and securely dispose of sensitive data.

Additionally, banks must share sensitive data with vendors and service providers, as certain outsourced functions are integral to their overall business strategy. This necessity, however, doesn't make sharing sensitive data with third parties any less complex or anxiety-inducing. Data breaches and leaks, even if they originate from a third party, can cause significant financial and reputational harm to banks. Alternatively, not sharing sensitive data with service providers can lead to higher operating costs and missed opportunities. That's why it's critical to carefully weigh the risks and benefits, consider a persistent protection solution, and make informed decisions about sharing sensitive data with third parties.

Borderless Security

Consider this scenario: An employee accidentally shares confidential information with the wrong vendor while working with multiple vendors simultaneously. The vendor may misuse this data, either intentionally or unintentionally, by sharing it with third parties, leading to malicious activities like printing fake documents, defrauding people, or publicizing the information. Unfortunately, the bank has no effective technical or legal means to prevent this and cannot deny the incident, resulting in long-term reputational damage. Solely relying on audits and legal actions is insufficient; banks need a systemic solution to securely outsource data without depending solely on signed agreements.

Vendors often don't have enough resources and fail to implement security and data protection strategies as robust as their contracting organizations, making audits challenging. Despite modern security measures like dynamic Firewalls, Intrusion Detection and Prevention Systems, and Data Loss Prevention (DLP) systems, vendors can still mishandle a bank's confidential information.

Data-centric security is the solution: This ensures that protection travels with digital assets, even after they're shared with vendors and other partners — providing complete visibility and control wherever those digital assets go — anywhere in the world. Data-centric security reinforces compliance with regulatory and legal frameworks like the RBI Guidelines by federating granular security policies throughout your organization and vendor networks.

Introducing Seclore

Almost all of the data created and transmitted by banks and their customers is sensitive to some degree and must be protected. With Seclore, banks can persistently protect digital assets so they can track and control sensitive data wherever it goes.

As cyber threats become more frequent and sophisticated, organizations must rethink their protection strategies. Relying on traditional perimeter-based security measures, which focus on network and device boundaries, leaves organizations vulnerable to account hijacking and human error. Organizations that focus on securing data in addition to perimeters can multiply their overall protection by embedding authentication, usage, and security controls alongside their most sensitive data.

Mapping Seclore Data-Centric Security to RBI Guidelines

Requirements

The Reserve Bank of India (RBI) has issued comprehensive guidelines to all Scheduled Commercial Banks (excluding regional rural banks), covering everything from information security to customer awareness programs. Formulated by the Working Group on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds, chaired by Shri G. Gopalakrishnan, RBI's Executive Director, these guidelines emphasize IT governance as an integral component of corporate governance. Indian banks are expected to rigorously adhere to this principle, highlighting data-centric security as playing a crucial role in complying with information security and outsourcing regulations.

How Seclore Helps

Seclore mitigates data leakage and unauthorized access by ensuring that sensitive digital assets are only accessible by authorized users. It also addresses loopholes and workarounds for Data Loss Prevention (DLP) solutions, such as password-protected files, ZIP, and encrypted files, that traditional DLP systems often miss. This holistic approach helps banks maintain data governance and regulatory compliance, ensuring that sensitive digital assets remain protected regardless of whom they are shared with.

This whitepaper explains how Seclore helps banks and financial institutions comply with all the guidelines issued by the Reserve Bank of India. It emphasizes how Seclore can assist organizations in this sector in adhering to specific sections of the RBI Guidelines issued over the years, ensuring efficient data governance and security.

Know Your Data

In banking, it is crucial to understand where personally identifiable information (PII), payment card information (PCI), and other sensitive data reside within an organization. Organizations must map all data repositories, databases, and storage systems that house personal and financial information to accomplish this. Implementing robust discovery classification tools can help identify and categorize sensitive data, which is the first step toward applying the appropriate level of protection. Banks must also establish stringent data governance policies to prevent data leakage, which include:

Data Inventory and Classification:
Conduct a detailed inventory to identify where sensitive customer data such as PII, PCI, and other financial information is stored. Use classification tools to categorize digital assets based on sensitivity and regulatory requirements.

Employee Training and Awareness:
Regularly train employees on data protection policies, the importance of data security, and best practices for preventing data leakage.

Incident Response Plan:
Develop and maintain a plan to quickly address and mitigate data breaches or leaks, minimizing impact.

Vendor Management:
Ensure that third-party vendors' handling of sensitive data adheres to the same protection standards you employ, including due diligence and regular audits of their security practices.

By implementing these measures, banks can significantly reduce the risk of data leakage and protect customer information from unauthorized access and breaches.

Data Classification

Requirements

2023 - Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices:

"REs shall ensure identification and mapping of the security classification (in terms of Confidentiality, Integrity, and Availability) of information assets based on their criticality to the REs' operations."

2018 - Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs):

"Classify data/information based on sensitivity criteria of the information. Appropriately manage and provide protection within and outside UCB/network, keeping in mind how the data/information is stored, transmitted, processed, accessed, and put to use within/outside the UCB's network and the level of risk they are exposed to depending on the sensitivity of the data/information."

2016 - Cyber Security Framework in Banks, 2016 - Baseline Cyber Security and Resilience Requirements:

"Classify data/information based on the bank's information classification/sensitivity criteria. Appropriately manage and provide protection within and outside organization borders/network, taking into consideration how the data/information are stored, transmitted, processed, accessed, and put to use within/outside the bank's network and the level of risk they are exposed to depending on the sensitivity of the data/information."

How Seclore Helps

Seclore's data-centric security protects digital assets on any network, machine, or device, ensuring they remain secure wherever they are accessed. It enables organizations to safely share sensitive data with outsourcing agencies and prevents that data from being misused or accessed by unauthorized users.

Seclore only allows authorized users to access protected digital assets from approved locations or devices. It also tracks access and usage activity to enhance visibility and promote enforcing data governance policies in third-party networks. Seclore also integrates seamlessly with data discovery and classification tools and can apply protection and usage controls to documents, emails, and attachments based on the applied label. Seclore Digital Asset Classification (DAC) manages data classification without encrypting it, ensuring that files cannot be copied or emailed to external addresses based on their classification.

Seclore's Solution Consulting team has decades of experience working with regulators and customers in this industry. The team engages, guides, and supports enterprise teams to help them understand the relative risk, value, and sensitivity of their organization's assets.

Audit Trails and SIEM Integration

Requirements

2023 - Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices:

"Every IT application that can access or affect critical or sensitive information shall have the necessary audit and system logging capability and should provide audit trails. The audit trails shall satisfy a Regular Entity's (RE) business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of the audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes. REs shall put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorized activity."

2023 - Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices

"Every IT application which can access or affect critical or sensitive information, shall have necessary audit and system logging capability and should provide audit trails. The audit trails shall satisfy a RE's business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes."

2019 - Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach

"Ability to know who did what, when, how, and preservation of evidence. Integration of various log types and logging options into a Security Information and Event Management (SIEM) system, ticketing/workflow/case management, unstructured data/big data, reporting/ dashboard, use cases/rule design."

How Seclore Helps

Seclore provides detailed audit trails and reports, including forensic-level telemetry, such as user, machine name, IP address, and related timestamps, so you always know who did what, when, and how. By Integrating Seclore with an SIEM or BI tool, admins can also enable automated alerts for suspicious activity.

Reports provide detailed information downloadable in Excel or other formats to ensure that sensitive data is secure across any network, machine, or device and that outsourcing remains safe.

Seclore Risk Insights dashboard offers complete visibility into sensitive digital asset usage and activity globally and seamless integration into enterprise SOC programs.

The system monitors all user activity related to protected digital assets, allowing information owners to modify or revoke access remotely at any time.

Protect Your Data

Understanding where sensitive data is stored inside and outside an organization is critical to preventing data leakage. Implementing comprehensive measures involves several key steps:

Data Access Controls:

Establish robust access control mechanisms to ensure only authorized users can access sensitive data. Utilize role-based access control (RBAC) to limit data access based on individual or team-based roles and responsibilities and regularly review and update access policies.

Data Encryption:

Encrypt sensitive data at rest and in transit using strong encryption standards like AES-256 to protect it from unauthorized access and ensure data confidentiality and integrity.

Data Loss Prevention (DLP) Systems:

Deploy a DLP to monitor and control data transfers across networks, endpoints, and cloud environments. These systems help detect and prevent unauthorized sharing and enforce data security policies.

Third-Party Vendor Management:

Ensure third-party vendors handling sensitive customer data adhere to stringent data protection standards. Conduct regular security assessments and audits to verify their compliance with data security policies and contractual obligations.

Banks can significantly reduce the risk of data breaches by tracking sensitive customer data and enforcing robust security protocols. These proactive measures help achieve compliance with data protection regulations and strengthen customer trust and confidence in the bank's commitment to data security.

Teleworking Controls

Requirements	How Seclore Helps
2023 - Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices *"Ensure that data/ information shared/ presented in teleworking is secured appropriately."*	Seclore-protected files give organizations complete control over who can access and perform specific actions on them. Information owners can also track changes made to files in real time, regardless of the file's location or device/platform from which they are accessed. Seclore eliminates the need to depend on third-party security infrastructure and legal agreements to protect sensitive data. With Seclore, information owners retain complete control over confidential information shared with third parties such as remote employees (teleworkers), vendors, partners, contractors, subcontractors, lawyers, and auditors.

Third-Party/Vendor Risk Management

Requirements	How Seclore Helps
2023 - Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices *"REs shall put in place an appropriate vendor risk assessment process and controls proportionate to the assessed risk and materiality:* • *Comply with applicable legal regulatory requirements and standards to protect customer data.* • *Manage supply chain risks effectively."* **2016 - Baseline Cyber Security and Resilience Requirements:** *"Banks shall be accountable for ensuring appropriate management and assurance of security risks in outsourced and partner arrangements. Among others, banks shall regularly conduct effective due diligence, oversight, and management of third-party vendors/service providers & partners."*	Seclore applies persistent encryption, authentication, and usage controls directly to digital assets rather than networks, devices, or perimeters so organizations can confidently share sensitive data with their partners. Now, organizations can protect and control sensitive data shared with partners and enforce their own data governance policies even after sharing digital assets containing sensitive data with third parties. Information owners can remotely revoke access when sharing sensitive data with outsourced agencies, partners, or contractors. This capability removes the need for third parties to comply with contract clauses, allowing organizations to effectively manage outsourcing and mitigate supply chain risks.

Access Control

Requirements	How Seclore Helps
2023 - Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices: *"Access to information assets shall be allowed only where a valid business need exists."*	Seclore restricts access to authorized users, applies granular usage controls, and lets organizations remotely enforce data governance policies. Thus, organizations can safely outsource and collaborate with partners while maintaining stringent data security standards. Organizations can instantly revoke access to any protected digital asset if unauthorized access is detected, reducing the need for third-party compliance.

Secure Mail and Messaging Systems

Requirements	How Seclore Helps
2018 - Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) **2016 - Cyber Security Framework in Banks** **2016 - Baseline Cyber Security and Resilience Requirements** *"Implement secure mail and messaging systems, including those used by bank's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links, etc."*	Seclore's data-centric security and granular usage controls (view, edit, print, share, screen share) can apply to sensitive data shared by email or uploaded/downloaded from the cloud. It can also protect data in cloud repositories like SharePoint, OneDrive, and Google Drive, applying security controls to documents even when shared externally from these environments.

Customer Data Protection

Requirements

2018 - Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs):

"UCBs, as owners of customer sensitive data, should take appropriate steps in preserving the Confidentiality, Integrity, and Availability of the same, irrespective of whether the data is stored/in transit within themselves or with the third-party vendors; the confidentiality of such custodial information should not be compromised in any situation. To achieve this, UCBs need to put suitable systems and processes across the data/information lifecycle in place. Regarding customers, UCBs may educate and create awareness among them about cyber security risks."

2016 - Cyber Security Framework in Banks:

"Banks depend on technology very heavily not only in their smooth functioning but also in providing cutting-edge digital products to their consumers and, in the process, collect various personal and sensitive information. Banks, as owners of such data, should take appropriate steps in preserving the Confidentiality, Integrity, and Availability of the same, irrespective of whether the data is stored/ in transit within themselves, with customers, or with third-party vendors; the confidentiality of such custodial information should not be compromised at any situation and to this end, suitable systems and processes across the data/information lifecycle need to be put in place by banks."

How Seclore Helps

Seclore provides data-centric security and precise usage controls (such as view, edit, print, share, and copy) that can be applied manually or automatically to sensitive digital assets shared on various platforms like email, cloud storage, FTP, or USB drive. It can also safeguard data in cloud repositories like SharePoint, OneDrive, and Google Drive, implementing security controls on assets even when shared externally from those environments. Only authorized users can access a protected file.

Data Leak Prevention

Requirements

2019 - Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach

2016 - Cyber Security Framework in Banks

2016 - Baseline Cyber Security and Resilience Requirements

"Develop a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information."

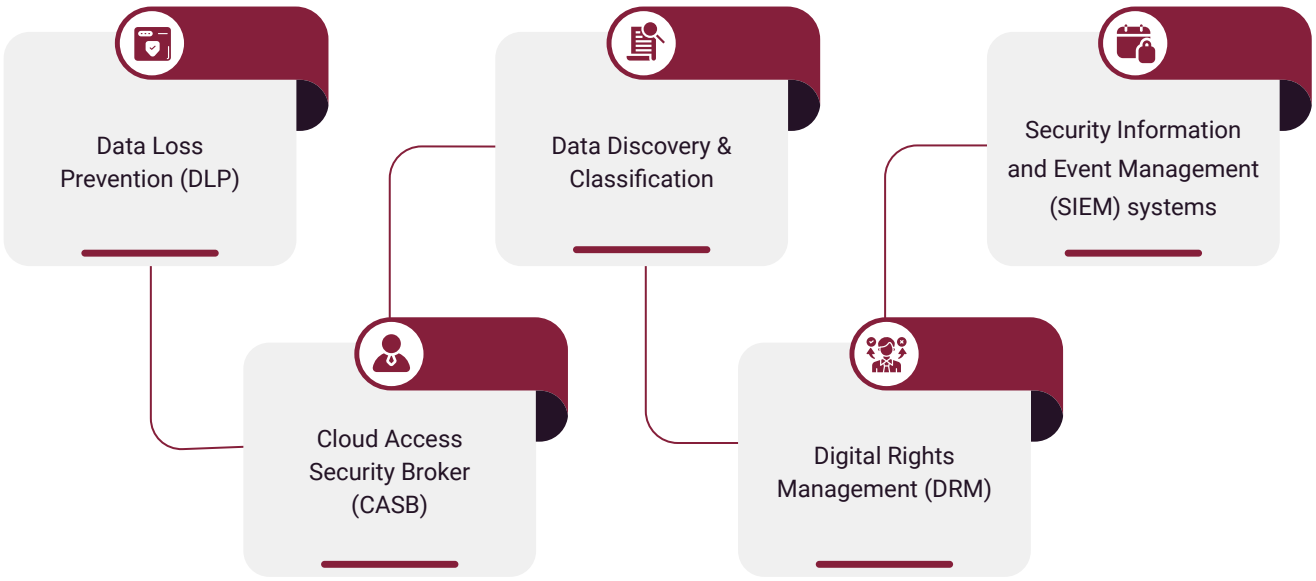
How Seclore Helps

Seclore integrates seamlessly with DLP solutions like Broadcom (Symantec®), Forcepoint, McAfee/Trellix, and Skyhigh. It also enhances the effectiveness of existing DLP and CASBs by automatically classifying and EDRM-protecting assets before they are shared. Seclore connectors supplement existing email and network DLP systems by securing shared assets (documents and emails) across various transmission layers.

Organizations rely on password protection, encryption, or ZIP files to safeguard confidential information before sharing it with outsiders. However, traditional DLP solutions cannot discover, classify, track, or monitor data in these formats, increasing the risk of sensitive information leaking and potentially leading to non-compliance.

Integrating Seclore with a DLP means the data can be decrypted for DLP scanning and re-encrypted before leaving the organization's perimeter. Seclore's comprehensive data-centric security enables organizations to know, protect, and control their customer's valuable information, safeguarding it from unauthorized access, breaches, and leakage.

The tools used to perform these functions include:



IT and Information Security Risk Management Framework

Requirements

2023 - Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices

"Identification of critical information systems of the organization and fortification of the security environment of such systems. Definition and implementation of necessary systems, procedures, and controls to ensure secure storage/ transmission/ processing of data/ information."

How Seclore Helps

Protecting sensitive digital assets with persistent encryption and granular usage controls means that the data in that asset remains secure, independent of its surrounding environment: the network, storage, transmission protocol, device, and other details are no longer a factor.

Seclore Risk Insights dashboard gives organizations more visibility for their sensitive data no matter where it travels. Using Seclore, organizations can monitor activity associated with Seclore-protected digital assets anywhere in the world. This granular usage and activity data can also be forwarded to the enterprise SOC program to provide a comprehensive view of organizational risk.

Control Your Data

Controlling sensitive customer data wherever it goes allows banks and other financial services organizations to confidently share sensitive data with partners. Leveraging advanced data encryption, access controls, and continuous monitoring systems, banks can ensure that sensitive information remains protected, whether stored internally, shared with third-party vendors, or transmitted across networks. This approach, known as "data-centric security," helps prevent unauthorized access and data breaches — safeguarding customer privacy and maintaining regulatory compliance.

Data Access Controls

Implementing strict access controls ensures that only authorized users can access sensitive data. Organizations can use role-based access controls (RBAC) to limit access based on job function, team, necessity, and other criteria.

Data Encryption

Encrypting sensitive data at rest and in transit helps mitigate unauthorized access, harm from breaches, and ensures data integrity.

Regular Audits and Monitoring

Conduct regular audits and continuous monitoring of data access and usage patterns to detect any unusual activity that may indicate a potential data breach.

Cryptographic Controls

Requirements	How Seclore Helps
2023 - Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices *"The key length, algorithms, cipher suites, and applicable protocols used in transmission channels, processing of data, and authentication purpose shall be strong. REs shall adopt internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable, and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions."*	Seclore natively supports multi-layered encryption utilizing several dimensions and parameters and custom or proprietary encryption. Seclore Enterprise Digital Rights Management (EDRM) includes two highly secure and compliant encryption algorithms, AES 256 and RSA 2048. Seclore EDRM protects all copies of a digital asset, regardless of the transfer mode - email, USB, shared folders, or any other method so digital assets remain protected even after sharing with external parties. The file-level firewall permits or blocks access based on predefined rules.

Straight-Through Processing

Requirements	How Seclore Helps
2023 - Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices *"To prevent unauthorized modification of data, REs shall ensure that data is not manually intervened in or modified while it is being transferred from one process to another or from one application to another, in respect of critical applications."*	Seclore-protected files are encrypted in transit, and data cannot be modified while being transferred from one endpoint or application to another. With Seclore, organizations have complete control over who, how, and when a user can access and edit a file. It also tracks and logs real-time changes regardless of the user's location, device, or platform.

Protect Your Information – Anytime, Anywhere

With customers like IDFC First Bank and HDFC Bank, Seclore's data-centric security solution has been proven to:

- Help banks protect their confidential information.
- Eliminate data leakage and theft, especially for outsourced business operations.
- Improve compliance and reporting capabilities with the relevant guidelines and auditors.

Know – Know where your sensitive customer data is and prevent sensitive data leakage.

Protect – Protect sensitive data from unauthorized access by applying granular usage controls.

Control – Track the use of information wherever it travels and automatically generate audit reports.

We're rapidly approaching a day when banks will face legal action and fines/penalties under the IT Act for data breaches originating from vendors or third parties (over which the bank has no control) and for the leakage of confidential information by employees.

Seclore's data-centric security platform allows enterprises to accurately classify, protect, track, and control every digital asset. This approach ensures that organizations can know, control, and protect their data wherever it goes, preventing data theft and ensuring compliance. With Seclore's data-centric security solution, Indian banks can comply with regulations and all relevant guidelines and ensure that the sensitive information they need to share with employees, partners, and outsourced business units for external collaboration remains safe and protected.

SECLORE™

About Seclore

Our mission is to safeguard sensitive information worldwide, regardless of its location. Seclore offers persistent protection and visibility for digital assets to help organizations remain secure and compliant. Our data-centric security approach ensures that only authorized individuals can access protected digital assets. With Seclore, organizations can specify who can access their data, what actions are permitted, and how long that access lasts. Join industry leaders like American Express in choosing Seclore for superior digital asset protection without sacrificing seamless collaboration and sharing.

Visit **seclore.com** for more information.

5201 Great America Parkway
Suite 440
Santa Clara, CA 95054