Compliance Brief

Data Security Compliance with Reserve Bank of India: Outsourcing of Information Technology Services Directions, 2023

cpl.thalesgroup.com

THALES

Building a future we can all trust

THALES
Building a future we can all trust

What is Outsourcing of Information Technology Services Directions, 2023 by RBI?

Indian Regulated Entities (REs) have been extensively leveraging Information Technology (IT) and IT enabled Services (ITeS) to support their business models, products and services offered to their customers. REs also outsource a substantial portion of their IT activities to third parties, which expose them to various risks.

To ensure effective management of attendant risks, the Reserve Bank of India finalized the Outsourcing of Information Technology Services Directions, 2023 on 10 April 2023 and shall come into effect from October 1, 2023.

Which organizations are subject to this Directions?

- Schedule Commercial Bank including Foreign Banks located in India, Local Banks, Small Finance Banks, and Payments Banks but excluding Regional Rural Banks;
- Primary (Urban) Co-operative Banks excluding Tier 1 and Tier 2 Urban Co-operative Banks;
- Credit Information Companies (CICs);
- Non-Banking Financial Companies ("NBFCs"); and
- All India Financial Institutions (EXIM Bank, NABARD, NaBFID, NHB and SIDBI).

The Directions have prescribed 9 control focuses with appendixes on the Usage of Cloud Computing Services, Outsourcing of Security Operations Centre and Services not considered under Outsourcing of IT Services.

When will the Directions be enforced?

RBI has given REs up to twelve months from the date of issuance of the Directions to re-visit their outsourcing arrangements and comply with the requirements enclosed under the Directions if such renewals are due before October 01, 2023, and has offered thirty-six months from the date of issuance of the Directions, if their agreements are due for renewal after October 01, 2023.

Definitions

Material Outsourcing of IT Services

The term 'material outsourcing of IT services' means any service which "if disrupted or compromised shall have the potential to impact the RE's business operations significantly"; or "may have a material impact on the RE's customers in the event of any unauthorized access, loss or theft of customer information.".

Implication:

1. This definition means that the IT Outsourcing Directions are meant for such REs especially NBFCs that undertake lending and other financial services only through digital means.
2. The definition is linked to access to customer data and its protection which means that the directions shall apply to any IT service agreement where there is access to customer data.

Outsourcing of IT Services shall include outsourcing of the following activities:

- IT infrastructure management, maintenance and support (hardware, software, or firmware);
- Network and security solutions, maintenance (hardware, software, or firmware);
- Application Development, Maintenance and Testing; Application Service Providers (ASPs) including ATM Switch ASPs;
- Services and operations related to Data Centres;
- Cloud Computing Services; and
- Management of IT infrastructure and technology services associated with the payment system ecosystem.

The remaining services which are not considered as Outsourcing of IT Services or are included in Appendix III shall be considered as outsourcing of financial services and shall not be covered under these IT Outsourcing Directions.

How Thales can help with the Outsourcing of IT Services Directions?

Thales helps REs comply with the Outsourcing of IT Services Directions 2023 by addressing two of the controls and the requirement for Usage of Cloud Computing Services.

CSP Managed Encryption Keys		Customer Managed Encryption Keys (CMEK)		
Default CSP Protection	**Managed CSP Protection**	**Bring Your Own Key (BYOK)**	**Hold Your Own Key (HYOK)**	**Bring Your Own Encryption (BYOE)**
CSP transparently handles key management and encryption of data without any customer involvement or control	CSP handles key management and encryption of data; with some customer monitoring, but no control	Customer generated and rotates keys using entropy and security policies of choice and then hands these keys to the CSP	CSP handles encryption of data but the key management is under customer control; directly or through third party key broker	CSP only stores encrypted data. Encryption and key management is done by a customer provided solution or third party

LOW Customer conrol over encryption and key management HIGH

The Directions	Thales Solutions
Chapter – VI: Risk Management | 17. Risk Management Framework	
REs shall seek to ensure the **preservation and protection of the security and confidentiality of customer information** in the custody or possession of the service provider. Access to customer information by staff of the service provider shall be on need-to-know basis." (f) "In the event of multiple service provider relationships where two or more service providers collaborate to deliver an end-to-end solution, the RE remains responsible for understanding and monitoring the **control environment of all service providers that have access to the RE's data, systems, records or resources.**"	CipherTrust Data Security Platform is an integrated suite of data-centric security products and solutions that unify data discovery, protection, and control in one platform. CipherTrust Platform provides multiple capabilities for protecting data at rest in files, volumes, and databases. Among them: • CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management and privileged user access control and detailed data access audit logging. It provides a complete separation of roles, where only authorized users and processes can view unencrypted data. This ensures privacy and protects sensitive data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. Data Security Fabric monitors data from a unified viewpoint for auditing across diverse on-premises and cloud platforms, providing oversight for relational databases, NoSQL databases, mainframes, big data platforms, and data warehouses. Detailed structured and unstructured data activity is captured automatically, making it easier to fulfill audit requests.
(i) The REs shall **review and monitor** the control processes and security practices of the service provider to **disclose security breaches**.	CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) continuously monitors processes for abnormal I/O activity and alerts or blocks malicious activity before ransomware can take complete hold of your endpoints and servers. It monitors active processes to detect ransomware – identifying activities such as excessive data access, exfiltration, unauthorized encryption, or malicious impersonation of a user, and alerts/blocks when such an activity is detected. Threat detection is one of the most important capabilities to prevent or identify and respond to a cyberattack. Imperva Data Security Fabric Threat Detection monitors data access and activity for all databases and provides the visibility needed to pinpoint risky data access activity for all users, including privileged users. REs can uncover hidden risks and vulnerabilities while creating reports to effectivelycommunicate risk and ongoing activities. It delivers real-time alerting and user access blocking of policy violations and cost-effectively retains years of data for audits.

Chapter – X: Exit Strategy

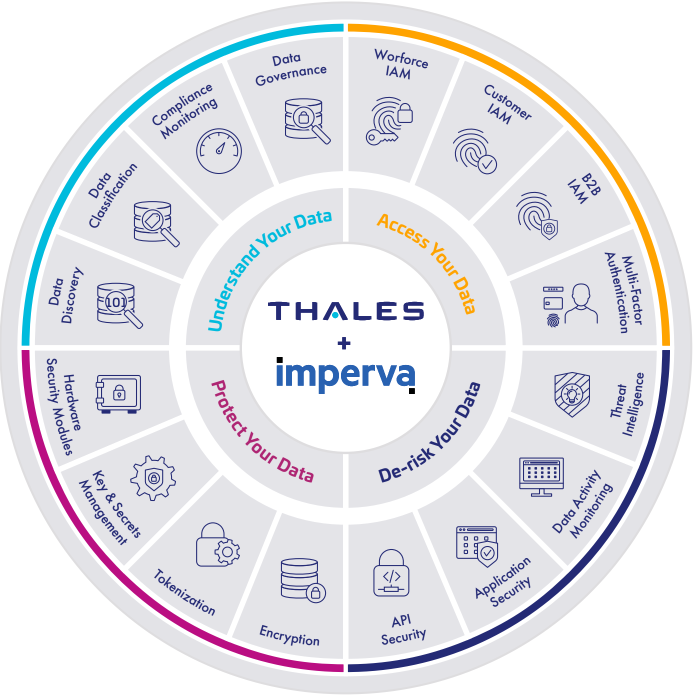
b) REs shall ensure that the agreement has necessary clauses on safe removal/ destruction of data, hardware and all records (digital and physical), as applicable.	REs can rely on **CipherTrust Enterprise Key Management** to remove encrypted information that managed by CSP effectively. Encrypted information can be effectively deleted by destroying encryption keys with **CipherTrust Enterprise Key Management**, it streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases.

Appendix – I | Usage of Cloud Computing Services

3. "...Cloud security is a shared responsibility between the RE and the Cloud Service Provider (CSP). REs may refer to some of the cloud security best practices, for implementing necessary controls, as per applicability of the shared responsibility model in the adoption of cloud services."	REs can take control of their cloud security and improve visibility with Thales **CipherTrust Cloud Key Management**. CipherTrust Cloud Key Management (CCKM) protects your time as well as your data with a single pane of glass view across regions for cloud-native, it offers one straightforward UI to manage all cloud Key Management Services (KMS). CCKM supports Bring Your Own Key (BYOK) use cases across multiple cloud infrastructures and SaaS applications. CCKM combines support for cloud provider BYOK APIs, cloud key management automation, and key usage logging and reporting, to provide cloud consumers with a cloud key management service that delivers strong controls over encryption key life cycles for data encrypted by cloud services. Hold Your Own Key (HYOK) further strengthens the level of control by REs, it offers a strong separation of duty for the encryption keys. The REs can maintain control of their keys instead of entrusting them to the CSP, they can achieve explicit and unambiguous delineation/ demarcation of responsibilities for all activities of the cloud services with CSP.
6. Cloud Services Management and Security Considerations **a. Service and Technology Architecture** - "REs shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to **globally recognised architecture principles and standards.**"	With extensive experience in helping financial institutions comply with industry mandates, Thales offers integrated encryption and key management solutions to protect cloud-based applications for REs with BYOE and BYOK. The bring-your-own-encryption (BYOE) is the best option for separation of trust between REs and the CSP. BYOE approach offers the ultimate separation of duty by allowing customers to use their own encryption as well as key management tools instead of the corresponding solutions offered by the CSP. This gives REs the highest level of control over their data, since the data and keys are never exposed to the CSP. Instead, data is encrypted before sending it to the CSP for storage. **Thales CipherTrust Transparent Encryption (CTE)** and **CipherTrust Tokenization** offer advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to ensure data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management. - **CipherTrust Transparent Encryption** allows REs to encrypt data and maintain control and compliance when moving data to the cloud or big data environments. Cloud providers cannot access token vaults or any of the keys associated with tokenization root of trust. - **CipherTrust Tokenization** tokenizes the data before it is migrated to the cloud in the obfuscated form to protect the data from any breach.

	Bring Your Own Key (BYOK) approach addresses the separation of duties between the CSP and REs to manage encryption keys in the cloud. The **CipherTrust Cloud Key Management** **(CCKM)** supports Bring Your Own Key (BYOK) use cases across multiple cloud infrastructures and SaaS applications. CCKM combines support for cloud provider BYOK APIs, cloud key management automation, and key usage logging and reporting, to provide cloud consumers with a cloud key management service that delivers strong controls over encryption key life cycles for data encrypted by cloud services.
• "… prefer a technology architecture that provides for **secure container-based data management**, where **encryption keys and Hardware Security Modules** are under the control of the RE."	**Thales** **Luna Hardware Security Modules** **(HSM)** allows organizations to have a dedicated Hardware for a greater degree of control and ownership over the crypto keys rather than with the Cloud Service Provider (CSP). HSM provides a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Available in three FIPS 140-3 certified form factors, Luna HSMs support a variety of deployment scenarios.
• "The architecture should provide for a standard set of tools and processes to manage containers, images and releases."	**CipherTrust Transparent Encryption Container Security** delivers in-container capabilities for encryption, access controls, and data access logging, so organizations can establish strong safeguards around data in dynamic container environments.
• "**Multi-tenancy environments** should be protected against data integrity and confidentiality risks, and against co-mingling of data." • "The architecture should be **resilient** and enable **smooth recovery** in case of failure of any one or combination of components across the cloud architecture…"	**CipherTrust Enterprise Key Management** offers multi-tenant and high availability for REs to meet the requirements. **CipherTrust Manager** is a high-availability appliance that centralizes encryption key management for the Thales Data Security Portfolio and third-party encryption solutions. CipherTrust Manager helps direct key life-cycle tasks including generation, rotation, destruction, import and export as well as provide abilities to manage certificates and secrets. Additionally, CipherTrust Manager offers multi-tenency, or domains, allowing customers and service providers to generate unique key management environments. This provides additional security and ultimate separation of duties, where no single administrator has access to all domains.
b. Identity and Access Management (IAM):	**Thales OneWelcome** identity and access management solutions limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensure the right user is granted access to the right resource at the right time. This minimizes the risk of unauthorized access. • **SafeNet Trusted Access** is a cloud-based access management solution that provides commercial, off-the-shelf multi-factor authentication with the broadest range of hardware and software authentication methods and form factors. • **Thales** **converged badge solutions** simplify the management of physical and logical access by consolidating all corporate security applications in a single user's badge: physical access to buildings and restricted areas, visual identification of the cardholder, secure access to sensitive digital resources thanks to PKI-certificate based and/ or FIDO authentication. • The broad list of **supported authentication methods** meets the needs of a large variety of users and enables organizations to protect all their users and sensitive digital resources with strong multifactor authentication.

Organizations can leverage Thales' suite of identity and data security solutions available on a single unified platform to become compliant today and stay compliant in the future. Contact us now!



About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us