cpl.thalesgroup.com

THALES
Building a future we can all trust

Addressing The Requirements of The Framework for Adoption of Cloud Services by SEBI Regulated Entities

Securities and Exchange Board of India (SEBI) has introduced the **Framework for the Adoption of Cloud Services by SEBI Regulated Entities* (REs)** in circular no. SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 on March 6, 2023, which sets baseline standards for security and regulatory compliances. This framework is a crucial addition to SEBI's existing guidelines on cloud computing and is designed to help REs implement secure and compliant cloud adoption practices.

Objective

- Highlight the key risks, and mandatory control measures that regulated entities (REs) need to put in place before adopting cloud computing.
- Set out the regulatory and legal compliances by REs if they adopt such solutions.

What is the Framework for the Adoption of Cloud Services by SEBI Regulated Entities (REs)?

- Lay out the risks unique to public cloud services to guide REs in developing their risk management strategy.
- Note some best practices for mitigating cloud-specific threats.
- A principle-based framework that covers nine key aspects

The circular also touches on which aspects cloud service providers and REs are responsible for, and which control measures might be shared between them, depending on their particular arrangement.

When would it implement?

- Enforce immediately for all new or proposed cloud onboarding assignments/projects of the Res with the introduction on March 6, 2023.
- REs should be in compliance with the framework within 12 months.

Who needs to comply?

All Stock Exchanges	All Clearing Corporations	All Depositories	All Stock Brokers through Exchanges, All Depository Participants through Depositories
All Mutual Funds / Asset Management Companies / Trustee Companies / Boards of Trustees of Mutual Funds / Association of Mutual Funds in India (AMFI)	All KYC Registration Agencies	All Qualified Registrars to an Issue / Share Transfer Agents	

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Required Principles	Thales Offerings
Principle 6: Security Controls | 6.2.9. Encryption and Cryptographic Key Management:	
(i) 1. Data-at-rest encryption	Protecting data at rest Thales offers multiple solutions for data at rest that can coexist with native encryption provided by Cloud Service Provider (CSP). • CipherTrust Transparent Encryption • CipherTrust Tokenization • CipherTrust Application Data Protection • CipherTrust Manager
(i) 2. Data-in-motion	• Thales High Speed Encryptors solutions secure data in motion as it moves across the network between data centers and headquarters, branch and satellite offices, to backup and disaster recovery sites, on premises and in the cloud. • CipherTrust Transparent Encryption encrypts files while leaving their metadata in the clear. In this way, CSP can perform their system administration tasks without gaining privileged access to the sensitive data residing on the systems they manage.
(ii) Ensure control of encryption and key management 1a & 1b. "Bring Your Own Key" (BYOK) & "Bring Your Own Encryption" (BYOE) approach shall be adopted	Adopting Bring Your Own Encryption (BYOE) & Bring Your Own Key (BYOK) • CipherTrust Cloud Key Manager supports Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) use cases across multiple cloud infrastructures and SaaS applications in a single interface. It provides a stronger separation of duty for the encryption keys, the RE can maintain control of their keys instead of entrusting them to the CSP. • CipherTrust Transparent Encryption provides transparent encryption and access control for data residing in Amazon S3, Azure Files and more. It also offers advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor encryption lock-in and ensure data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management.
(ii) 3. Generating, storing and managing the keys in a Hardware Security Module (HSM) shall be implemented in a dedicated HSM	Protection of cryptographic keys Thales Luna Hardware Security Modules (HSM) allow organizations to have dedicated Hardware for a greater degree of control and ownership over the crypto keys rather than with the Cloud Service Provider (CSP).
6.2.12. Backup and recovery solution:	
(iii) Adopt encryption solutions and Key management.	Thales Cipher Trust Cloud Key Manager (CCKM) provides key lifecycle management along with automatic key rotation, recovery and key revocation feature that is not available by any cloud provider's managed Key Management System (KMS).
Principle 9: Vendor Lock-In and Concentration Risk Management | 9. Concentration Risk Management	
(ii) RE shall explore the option of cloud-ready and CSP agnostic solutions (iii) implement data portability and inter-operability as part of exit/ transfer strategy.	The challenge of BYOK and cloud key management depends on the number of clouds and keys organizations need to manage. • CipherTrust Cloud Key Manager combines support for cloud provider BYOK service, cloud key management automation, and key usage logging and reporting, to provide cloud consumers with strong controls over the encryption key life cycles for data encrypted by a cloud service provider. • Thales CipherTrust Transparent Encryption (CTE) and CipherTrust Tokenization offer advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor encryption lock-in.
10. Recommendations	
v. there should be a clear delineation and fixing of responsibility between the RE and the CSP	With HYOK, RE can achieve explicit and unambiguous delineation/ demarcation of responsibilities for all activities of the cloud services with CSP. 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).