FUTUREX

In accordance with *SEBI Guidelines/Framework*

KEY POINTERS FROM SEBI FOR ADOPTION OF CLOUD SERVICES

SEBI, the Securities and Exchange Board of India, has recently introduced a pivotal framework, outlined in circular no. SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 6, 2023. This framework establishes essential security and regulatory compliance standards for SEBI Regulated Entities (REs) utilizing cloud services. This framework represents a significant enhancement to SEBI's existing directives regarding cloud computing and serves as a guiding force for REs to embrace cloud adoption practices seamlessly and securely.

This framework is designed to illuminate the critical risks inherent in cloud computing adoption that require diligent attention from REs. By emphasizing mandatory control measures, the framework serves as a comprehensive roadmap for REs to implement before adopting cloud computing. Furthermore, the framework delineates the precise regulatory and legal compliance obligations that REs must adhere to should they choose to integrate cloud solutions into their operations.

Futurex stands ready with integrated solutions tailored to empower your organization in effectively addressing the imperatives laid out in the Framework for the Adoption of Cloud Services. Our solutions concentrate on two essential principles: Security Control and Concentration Risk Management.

Regulation Overview

The circular outlining the Framework for the Adoption of Cloud Services serves as a comprehensive guideline, addressing the distinct risks associated with public cloud services. This directive empowers REs to formulate a robust risk management strategy while highlighting effective practices to mitigate cloud-specific vulnerabilities. A pivotal emphasis lies in establishing requisite security measures; failure to do so, as advised in the circular, could render cloud-stored data susceptible to compromise by malicious entities. Consequently, security breaches could disrupt REs' operational continuity and impede their legal obligations.

The framework operates on a principle-based structure, encompassing some key dimensions outlined as follows:

- Crafting a public cloud risk management strategy that accounts for the distinctive attributes of public cloud services.
- Enforcing stringent controls in domains including cyber security, data safeguarding, and cryptographic key management.
- Expanding the purview of cyber security operations to encompass safeguarding public cloud workloads.
- Orchestrating cloud resilience strategies while addressing concerns like outsourcing, vendor dependency, and concentration risks.
- Ensuring the proficiency of personnel in managing public cloud workloads and associated risks.

Introduced on March 6, 2023, the Framework for the Adoption of Cloud Services by SEBI REs complements SEBI's existing array of circulars, guidelines, and advisories. It immediately affects all novel or proposed cloud onboarding initiatives undertaken by REs. Concurrently, existing cloud-service-adopting REs must align their arrangements with the framework within 12 months.

This framework charts the path towards secure and compliant cloud adoption practices, fortifying the integrity of REs' operations, ensuring their steadfast commitment to regulatory standards, and ensuring staff have the skills to manage public cloud workloads and risks.

How Futurex can Help

Futurex offers integrated solutions that enable your organization to address the Framework for adopting Cloud Services, focusing on Data Security, Security Control, and Key Management.

Protecting data at rest

Futurex offers multiple solutions for data at rest that can coexist with native encryption provided by Cloud Service Provider (CSP).

- ***File Encryption:*** Futurex provides HSMs, Key Management Servers, Cryptographic Management Platforms, and Cloud-based services. When you encrypt the file and control the key, your cloud provider cannot access it.
- ***Futurex Application Data Protection:*** Application encryption is a full-service cryptographic functionality available through the Key Management Enterprise Server (KMES) Series 3, incorporating general-purpose data encryption and key management technology into applications. Application encryption allows organizations to encrypt entire files or specific fields of data at the application level before it is stored.

- ***Futurex Key Manager:*** Futurex's Key Management Enterprise Server (KMES) Series 3 is a robust and scalable key management solution. It unites every possible encryption key use case from root CA to PKI to BYOK. Automate and script key lifecycle routines. Secure private keys with a built-in FIPS 140-2 Level 3 validated HSM. Deploy it on-premises for hands-on control or in the cloud for native integration with public cloud providers. The KMES Series 3 is the last word on encryption key management, the cornerstone of enterprise cryptographic ecosystems worldwide.

Adopting Bring Your Own Encryption (BYOE) & Bring Your Own Key (BYOK)

Futurex KMES (Key Management and Encryption Service): Futurex's cloud key management platform is powered by the KMES Series 3, a robust, easy-to-use solution for managing large volumes of keys, certificates, and other cryptographic objects. The KMES complies with all major security standards for HSMs, including PCI HSM and FIPS 140-2 Level 3.

A high-performance cryptographic module powers the KMES Series 3 and can rapidly generate symmetric secret keys and asymmetric PKI through its easy-to-use interface and API. The process of creating keys can be fully automated, so once the functionality is set up within the host system, an organization can be on its way to secure data storage and reduce compliance scope and cost. Offers comprehensive support for both Bring Your Own Key (BYOK) and Bring Your Own Encryption (BYOE) scenarios across various cloud infrastructures and Software as a Service (SaaS) applications through a unified interface. It delivers essential features such as key auditing, robust key generation, end-to-end key lifecycle management, and unique capabilities like automated key rotation, recovery, and key revocation, which are not typically found in cloud providers' managed Key Management Systems (KMS).

The BYOK and BYOE functionalities establish a more robust separation of duties concerning encryption keys, empowering the Responsible Entity to maintain control over their keys instead of relying on the CSP for this critical security aspect.

FUTUREX

For over 40 years, Futurex has been an award-winning leader and innovator in the encryption market, delivering uncompromising enterprise-grade data security solutions. Over 15,000 organizations worldwide trust Futurex to provide groundbreaking hardware security modules, key management servers, and cloud HSM solutions.

Futurex is headquartered outside of San Antonio, Texas, with regional offices worldwide and over a dozen data centers across five continents, Futurex delivers unmatched support for its clients' mission-critical data encryption and key management requirements.

FUTUREX.COM

864 Old Boerne Road,
Bulverde, Texas 78163