Fortanix

How Fortanix helps meet APRA CPS 230 guideline?

Eliminate Data Loss, Enable Business Continuity and Operational Resilience with Confidential Computing Powered Cryptography Service

What is APRA CPS 230?

> "APRA CPS 230 is a critical prudential standard that focuses on operational risk management within the Australian financial services industry. By adhering to its guidelines and requirements, APRA-regulated entities can enhance their operational resilience, minimize disruptions, and protect the interests of their customers and stakeholders."

In managing technology risks, an APRA-regulated entity must monitor the age and health of its information assets and meet the requirements for information security as mentioned in Prudential Standard CPS 234 Information Security (CPS 234). (Refer: Page 6 Operational Risk Management)

APRA CPS 230 guideline also talks extensively about business continuity

• Article 34 states: Organizations to maintain a credible Business Continuity Plan (BCP) that sets out how it would maintain its critical operations within tolerance levels through disruptions, including disaster recovery planning for critical information assets.

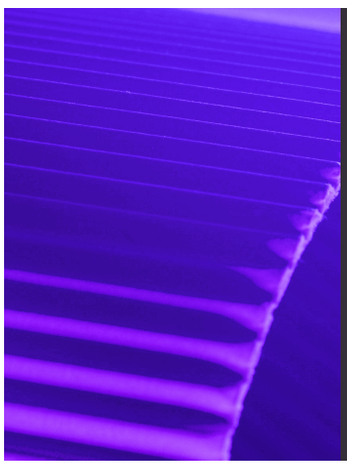
• Article 41. An APRA-regulated entity must maintain the capabilities required to execute the BCP, including access to people, resources, and technology.

Why Ensuring Data Confidentiality, Availability and Integrity is Critical for Business Continuity?

Data is the most valuable resource that an organization holds. Ensuring data availability is critical for the business continuity of an organization. Losing access to mission-critical data could bring your operations to a complete standstill resulting in financial loss and loos of reputation to your organization. Data breaches are the most common reason for data loss.

Cryptography or encryption is now commonly used by organizations to protect data confidentiality (preventing unauthorized viewing) and data integrity (preventing unauthorized changes).

ENCRYPTION IS EASY, KEY MANAGEMENT IS HARD Most organizations rely on encryption to protect sensitive data, but they are still struggling to get the key management right. If you lose the encryption key you loose any data that was encrypted by that key. Managing your keys securely is therefore critical to prevent data breaches and ensure business continuity



> "The proper management of cryptographic keys is essential to the effective use of cryptography for security. Keys are analogous to the combination of a safe. If a safe combination is known to an adversary, the strongest safe provides no security against penetration. Similarly, poor key management may easily compromise strong algorithms."
>
> NIST Recommendation for Key Management

That is why encryption key management should be one of your top priorities as far as data security and business continuity are concerned.

info@fortanix.com | 3910 Freedom Circle Suite 104, Santa Clara, CA 95054, United States

Why Confidential Computing is the Ultimate Solution?

Confidential computing protects data and applications by running them in secure enclaves or Trusted Execution Environment (TEE) that isolate the data and code to prevent unauthorized access, even when the compute infrastructure is compromised. Intel® SGX technology represents one of the leading implementations of Confidential Computing. Using Intel® SGX allows organizations to isolate the software and data from the underlying infrastructure (hardware or OS) by means of hardware-level encryption.

Implication: Confidential Computing offers the ultimate solution for ensuring data confidentiality, integrity, and availability. Organizations can now run sensitive applications and data on untrusted infrastructure, public clouds, and all other hosted environments. This gives organizations greater control over the security and privacy of applications and data inside and outside of their established security perimeter.

Drive outcomes with Fortanix

Integrated security

Fortanix provides secure key management and cryptography service across public, private, hybrid or multicloud environments, simplifying provisioning and control of encryption keys.

Data protection, whatever its state

Fortanix manages and enforces security policies including identity verification, data access control, and attestation to ensure the integrity and confidentiality of data, code, and applications.

Highly available key management service

The service is purpose-built for high availability — even if most nodes in a cluster are active. An ideal multi-site deployment of Fortanix would cover at least three data centres/KMS clusters (availability zones) to ensure high service availability. Keys are replicated within a cluster for the region.

Powered on Confidential Computing

Fortanix cryptography service is powered on Confidential Computing technology enabling organizations to secure data across its lifecycle-including in rest, transit and in use.

Secure encryption key storage

FIPS 140-2 Level 3 certified HSM to store encryption keys and cryptographic operations are securely executed within the module

For more details on Information Security Controls offered by Fortanix to help meet APRA guidelines like CPS 234/235

Download your Whitepaper