cpl.thalesgroup.com

THALES
Building a future we can all trust

Address Information Security Requirements of ASIC Market Integrity Rules in Australia

What are ASIC Market Integrity Rules?

ASIC introduced the ASIC Market Integrity Rules (Securities Markets and Futures Markets) Amendment Instrument 2022/74 which amends the **ASIC Market Integrity Rules (Securities Markets and Futures Markets) 2017**. The background on the amendments can be found in Report 719: Response to submissions on CP 314 Market integrity rules for technological and operational resilience.

The **Technological and operational resilience rules** commence on 10th March 2023 which set minimum expectations and controls to mitigate technological risks and help to safeguard the integrity and resilience of Australia's markets. The Rules also:

- Introduce additional obligations on market participants and operators in relation to technological and operational resilience
- Reinforce the broader regulatory focus on deterring inadequate systems and operational governance and controls
- Create greater alignment with international standards and other domestic standards
- Add to existing requirements on entities in respect of information security and operational resilience, such as APRA's Prudential Standard CPS 234: Information Security.

Who is ASIC?

Australian Securities & Investments Commission (ASIC) is Australia's integrated corporate, markets, financial services and consumer credit regulator. It is an independent Australian Government body and sets up under and administers the Australian Securities and Investments Commission Act 2001 (ASIC Act), and carries out most of the work under the Corporations Act.

Who needs to comply with ASIC Market Integrity Rules?

- Securities markets: ASX, Chi-X, NSXA, SSX and their participants
- Futures markets: ASX 24, FEX and their participants

How can Thales help with ASIC Market Integrity Rules Compliance?

Thales helps organizations comply with ASIC Market Integrity Rules by addressing Information Security Requirements for the market participants.

ASIC Integrity Rules	Thales Solution
8A.4.1 & 8B.3.1 Information security	
2a. arrangements to **identify and document Information Assets** that are integral to the provision of the Operator's Market Operations and Market Services	• **CipherTrust Data Discovery and Classification** efficiently identifies structured as well as unstructured sensitive data. Supporting both agentless and agent-based deployment models, the solution provides built-in templates that enable rapid identification of regulated data, highlight security risks, and help you uncover compliance gaps.
2b. **controls**, including automated controls, designed to **prevent unauthorised access** to Information Assets; and	• **Thales OneWelcome** identity & access management products and 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 ensuring that the right user is granted access to the right resource at the right time; whereby minimizing the risk of unauthorized access. • **SafeNet IDPrime smart cards** can be leveraged for implementing physical access to sensitive facilities. These smart cards can also augment Passwordless authentication initiatives relying on PKI and FIDO technology. • **CipherTrust Data Security Platform** enforces very granular, least-privileged-user access management policies, enabling protection of data from unauthorized access by privileged users or attackers. • **CipherTrust Transparent Encryption** encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. It provides a complete separation of roles where only authorized users and processes can view unencrypted data and to ensure a better control over the information assets. • **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.
2c. **controls** for identifying, assessing, **managing and monitoring for unauthorised access** to Information Assets	• **Thales OneWelcome** identity & access management solutions help to identify and authenticate users. It allows organizations to limit the access to confidential resources through use of MFA and granular access policies. • **SafeNet Trusted Access** allows organizations to respond and mitigate risks by providing an immediate, up to date audit trail of all access events to all systems. Extensive automated reports document all aspects of access enforcement and authentication. In addition, the service automatically streams logs to external SIEM systems. • **CipherTrust Data Security Platform** can enforce very granular, least-privileged-user access management policies, enabling the protection of data from misuse by privileged users and APT attacks. • **CipherTrust Transparent Encryption** solution protects data with file and volume level data-at-rest encryption, access controls, and data access audit logging without re-engineering applications, databases, or infrastructure. **MFA for CipherTrust Transparent Encryption** prompts system administrators and privileged users to demonstrate additional factors beyond a password before gaining access to sensitive data, to minimize the chance of a rogue user getting through. • **CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP)** provides a non-intrusive way of protecting files/folders from ransomware attacks. CTE-RWP watches for abnormal I/O activity on files hosting business-critical data on a per-process basis. It allows administrators to alert/block suspicious activity before ransomware can take hold of your endpoints/servers.

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.

> cpl.thalesgroup.com <

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