cpl.thalesgroup.com

THALES
Building a future we can all trust

Comply with the APRA Prudential Standard CPS234 in Australia

APRA Prudential Practice Guideline (PPG) to comply with CPS234

What is APRA Prudential Practice Guideline (PPG)?

The purpose of **Prudential Practice Guidelines (PPG)** is to provide guidance to Boards, senior management, risk management and information security specialists (both management and operational) of APRA-regulated entities with respect to the implementation of **Prudential Standard CPS234** Information Security. The multiple audiences reflect the pervasive nature of information security threats and vulnerabilities and the need for sound practices and a solid business understanding to maintain an information security capability in line with those threats and vulnerabilities.

Who needs to comply with CPS234?

CPS234 applies to APRA-regulated entities namely:

- Authorized deposit-taking institutions (ADIs), including foreign ADIs, credit unions, and banks
- General insurers
- Life companies and friendly societies
- Private health insurance companies
- Non-operating holding companies
- Superannuation funds

Who is APRA?

The Australian Prudential Regulation Authority (APRA), established by the Australian Government on 1 July 1998, is an independent statutory authority that supervises institutions across banking, insurance and superannuation, and is accountable to the Australian Parliament.

What is CPS234?

CPS234 is an information security law intended to ensure that regulated entities can withstand cyberattacks and other security threats. In addition, when an obvious data breach or other security incident is discovered, businesses must respond in a timely manner.

How can Thales help with CPS234 Compliance?

Thales helps organizations comply with CPS234 by addressing APRA Prudential Practice Guidelines (PPG) on Information Security Capability, Policy Framework, Information Asset Identification and Classification, implementation of controls and Incident management.

Prudential Practice Guidelines (PPG) for CPS234	Thales Solution
Guidelines 18 - INFORMATION SECURITY CAPABILITY: Capability of third parties and related parties	
INFORMATION SECURITY CAPABILITY: CAPABILITY OF THIRD PARTIES AND RELATED PARTIES **Guidelines 18** APRA's expectation is that an APRA- regulated entity would take reasonable steps to satisfy itself that the **third party** has sufficient information security capability to manage the additional threats and vulnerabilities resulting from such arrangements.	• With the **CipherTrust Data Security Platform (CDSP)**, administrators can create a strong separation of duties between privileged administrators and data owners. CDSP can also enforce very granular, least-privileged-user access management policies, enabling the protection of data from misuse by privileged users. • **CipherTrust Transparent Encryption** provides a complete separation of administrative roles, so only authorized users and processes can view unencrypted data. Unless a valid reason to access the data is provided, sensitive data stored in a third-party cloud provider will not be accessible in cleartext to unauthorized users. These could include third-party cloud provider employees, such as support engineers, DB admins, or potentially malicious processes. • **Thales OneWelcome Identity platform**'s fine-grained authorization capability helps organizations by providing the right amount of access to the right people at the right time. Its' delegation management capability empowers organizations to manage third-party identity efficiently.
Guidelines 21 – POLICY FRAMEWORK: A policy hierarchy informed by a set of key principles	

Guidelines 21 (a)
 	
identification, authorisation and granting of access to information assets (refer to Attachment C for further guidance)
	• **Thales OneWelcome Identity platform** limits 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 that the right user is granted access to the right resource at the right time; whereby minimizing the risk of unauthorized access. The platform brings support for a varieties of authentication methods including FIDO 2.0 and Passkeys. Fine-grained authorization functions enable complex B2B customer and consumer access control use cases.
	• **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 Transparent Encryption** with MFA feature limits privileged users' sensitive data.
	  ◦ **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.
	  ◦ Organizations can add an additional layer of protection with a second identity verification step at the access point with Multi-Factor Authentication (MFA) for CipherTrust Transparent Encryption.

Guidelines 21 (b) Life-Cycle Management that addresses the various stages of an information asset's life to ensure that information security requirements are considered at each stage, from planning and acquisition through to decommissioning and destruction	• **CipherTrust Enterprise Key Management** is a cost-effective and time-saving way to decommission/ destruct information no longer needed, by simply removing access to the decryption key from the system. It simplifies the administrative challenges around encryption key management to ensure that keys are secure and always provisioned to authorized encryption services.
Guidelines 21 (c) Management of information security technology solutions that include firewall, anti-malicious software, intrusion detection/ prevention, cryptographic systems and monitoring/ log analysis tools	• **Thales Luna Hardware Security Modules (HSMs)** provide the highest level of encryption security by always storing cryptographic keys in hardware. Thales HSMs provide a secure crypto foundation, as the keys never leave the intrusion-resistant, tamper-evident, FIPS-validated appliance. Strong access controls prevent unauthorized users from accessing sensitive cryptographic material because all cryptographic operations occur within the HSM. • **CipherTrust Manager** manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, supports robust auditing and reporting, and offers developer-friendly REST API. It allows organizations to limit user access to information systems that contain sensitive Information. It is available in both virtual and physical appliances that integrates with FIPS 140-2 compliant Thales Luna or third-party Hardware Security Modules (HSMs) for securely storing keys with the highest root of trust.

Prudential Practice Guidelines (PPG) for CPS234	Thales Solution
Guidelines 21 (d) Definition of an overarching information security architecture that outlines the approach for designing the IT environment (encompassing all information assets) from a security perspective e.g. authentication, identity management	• **CipherTrust Manager** offers streamlined and strengthened key management in cloud and enterprise environments over diverse use cases. Leveraging FIPS 140-2-compliant virtual or hardware appliances, it delivers high security to sensitive environments and centralizes key management for home-grown encryption, as well as third-party applications. It supports two-factor authentication for administrative access. • **Thales OneWelcome Identity Platform** allows organizations to associate devices and other digital identities with primary accounts, authenticate, authorize, collect, and store information about external and internal identities from across many domains. 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.

Guidelines 21 (k)
 	
mechanisms to assess compliance with, and the ongoing effectiveness of, the information security policy framework
	• Audit trail of **CipherTrust Data Security Platform** allows risk owners and auditors to assess and demonstrate compliance against the information security policy framework.
	  ◦ **CipherTrust Transparent Encryption (CTE)** that delivers detailed data access audit logs CipherTrust Security Intelligence (CSI) with logs and reports streamline compliance reporting
	  ◦ **CipherTrust Security Intelligence (CSI)** logs and reports streamline compliance reporting and speedup threat detection using leading Security Information and Event Management (SIEM) systems.

Guidelines 26 – INFORMATION ASSET IDENTIFICATION AND CLASSIFICATION: Classification of all information assets by criticality and sensitivity	
Guidelines 26 A thorough understanding of an APRA-regulated entity's information assets and the impact of a security compromise of those assets is important to maintain effective information security.	• Classify all information assets by criticality and sensitivity with **CipherTrust Data Discovery and Classification**, it offers complete visibility into your sensitive data with efficient data discovery, classification, and risk analysis across heterogeneous data stores - the cloud, big data, and traditional environments - in your organization.
Guidelines 36 – IMPLEMENTATION OF CONTROLS: Information security controls implemented at all stages	
Guidelines 36 (c): Deployment and Environment Management – development, test and production environments are appropriately segregated and enforce separation of duties	• **CiphterTrust Manager** centrally manages encryption keys and configures security policies so organizations can control and protect sensitive data with the separation of duties. • **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 complete separation of roles where only authorized users and processes can view unencrypted data.
Guidelines 36 (d): Access Management Controls – only **authorised users are able to access** information assets (refer to Attachment B for further guidance)	• **Thales OneWelcome identity & 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 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.
Guidelines 36 (e): Hardware and software asset controls – **appropriate authorisation** to prevent security compromises from unauthorised hardware and software assets	• **Digital Signing** for a wide range of applications with **Hardware security modules (HSMs)** protects the private keys used for secure electronic signatures; it enhances security and ensures compliance. • **Thales OneWelcome Identity Platform** facilitates external IoT device identity management via the OAuth2 Device Flow specification. Web-connected and user input-constrained devices can be linked with user identity accounts managed by OneWelcome tenants. Organizations can see and, if desired, disconnect paired devices. It also supports IoT device management in the B2B context.

Prudential Practice Guidelines (PPG) for CPS234	Thales Solution

Guidelines 36 (m): Service provider and Management Controls
 	
Ensure that a regulated entity's **information security requirements** are met.
	• **CipherTrust Data Security Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases. Among them:
	  ◦ **CipherTrust Transparent Encryption** allows organizations encrypt data and maintain control and compliance when moving data to the cloud or big data environments. Service providers have no access to token vaults or any of the keys associated with tokenization root of trust.
	  ◦ **CipherTrust Tokenization** permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data without exposing sensitive data during the analysis or in reports.
	  ◦ **CiphterTrust Manager** streamlines and strengthens key management in enterprise environments over a diverse set of use cases, it delivers high security to sensitive environments and centralizes key management for home-grown encryption, as well as third-party applications.
	• **Thales OneWelcome Identity Platform** tracks identity events and provides analytics reports, including failed login attempts, user profile changes, changes to credentials and devices, consent grants and revocations, changes to group memberships, etc.

MINIMISE EXPOSURE TO PLAUSIBLE WORST CASE SCENARIOS
 	
Guidelines 44
 	
APRA-regulated entities could consider low likelihood scenarios, which could result in an extreme impact to the regulated entity (i.e. plausible worst case) including:
• malicious acts by an insider with highly-privileged access, potentially involving collusion with internal or external parties;
• deletion or corruption of both production and backup data, either through malicious intent, user error or system malfunction; and
• loss of, or unauthorised access to, encryption keys safeguarding extremely critical or sensitive information assets.
	• **Hardware security modules (HSMs)** safeguard the cryptographic keys used to secure applications, and sensitive data, it enhances security and ensures compliance.
	• **CipherTrust Data Security Platform** can enforce very granular, least-privileged-user access management policies, enabling protection of data from misuse by privileged users and APT attacks.
	  ◦ **CipherTrust Transparent Encryption** encrypts files, while leaving their metadata in the clear. In this way, IT administrators -- including hypervisor, cloud, storage, and server administrators -- can perform their system administration tasks, without being able to gain privileged access to the sensitive data residing on the systems they manage.
	  ◦ **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.
	  ◦ **CipherTrust Manager** offers centralized Administration and Access Control, which unifies key management operations with role-based access controls. Authenticates and authorizes administrators and key users using existing AD and LDAP credentials. Prevents unauthorized password changes and alerts on simultaneous logins by the same user.
	• **Thales OneWelcome Identity Platform** allows organizations to virtually (or logically) limit access to confidential resources through the use of MFA (including phishing-resistant authentication) and granular access policies. 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.

PHYSICAL AND ENVIRONMENTAL CONTROLS **Guidelines 46 (b)** Physical access controls that protect the site perimeter, building, data room and computing racks. Common controls include gates, locks and procedures for granting and reviewing access by staff, third party providers and visitors	• **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.

Prudential Practice Guidelines (PPG) for CPS234	Thales Solution

CRYPTOGRAPHIC TECHNIQUES TO RESTRICT ACCESS
 	
Guidelines 54
 	
Cryptographic techniques can be used to control access to sensitive data, both in storage and in transit. The strength of the cryptographic techniques deployed would be commensurate with the sensitivity and criticality of the data as well as other supplementary or compensating controls (refer to Attachment E for further guidance).
	• **Hardware security modules (HSMs)** provide the highest level of encryption security by always storing cryptographic keys in hardware, and offer strong access controls prevent unauthorized users from accessing sensitive cryptographic material.
	• Thales's portfolio of **certificate-based authentication** form factors offers strong multi-factor authentication, enabling organizations to address their PKI security needs. Thales PKI tokens and smart card portfolio offer a single solution for strong authentication and applications access control, including remote access, network access, password management, network logon, as well as advanced applications including digital signature, data and email encryption.
	
	Protect Data in Transit/ Motion
	
	• **Thales High Speed Encryptors (HSEs)** provide network independent data-in-transit/ motion encryption (Layers 2,3 and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back.
	• **CiphterTrust Manager** centrally manages encryption keys and configures security policies so organizations can control and protect sensitive data with the separation of duties.
	
	Protect Data in use
	
	• **CipherTrust Vaultless Tokenization** protects data at rest while its policy-based Dynamic Data Masking capability protects data in use. A RESTful API in combination with centralized management and services enables tokenization implementation with a single line of code per field. Vaultless Tokenization is provided by dedicated, distributed-cluster-capable Tokenization Servers, offering full separation of duties.
	
	Protect Data At Rest
	
	• **CipherTrust Data Security Platform** safeguards and audits the integrity of customer records and information against a broad range of threats to data.
	  ◦ Thales' **CipherTrust Transparent Encryption** 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. Policy and encryption key management are provided by **CipherTrust Manager**.
	  ◦ **CipherTrust Tokenization** delivers capabilities for database tokenization and dynamic display security and secures pseudonymizing sensitive assets—whether they reside in data center, big data, container or cloud environments.
	  ◦ **CipherTrust Application Data Protection** delivers key management, signing, and encryption services enabling comprehensive protection of files, database fields, big data selections, or data in platform-as-a-service (PaaS) environments.

INFORMATION SECURITY TECHNOLOGY SOLUTIONS **Guidelines 56** An APRA-regulated entity would typically deploy appropriate information security technology solutions which maintain the security of information assets. Examples include firewalls, network access control, intrusion detection/prevention devices, anti-malware, encryption and monitoring/ log analysis tools	

Prudential Practice Guidelines (PPG) for CPS234	Thales Solution

END-USER DEVELOPED/ CONFIGURED SOFTWARE
 	
Guidelines 58
 	
An APRA-regulated entity would typically introduce processes to **identify and classify end-user developed/ configured software and assess risk** exposures. In APRA's view, any information software asset that is critical to achieving the objectives of the business or that processes sensitive data would comply with the relevant life-cycle management controls of the regulated entity.
	Protect Sensitive Data At Rest
	
	• **CipherTrust Data Security Platform** safeguards and audits the integrity of customer records and information against a broad range of threats to data.
	  ◦ Thales' **CipherTrust Transparent Encryption** 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. Policy and encryption key management are provided by **CipherTrust Manager**.
	  ◦ **CipherTrust Tokenization** delivers capabilities for database tokenization and dynamic display security and secures pseudonymizing sensitive assets—whether they reside in data center, big data, container or cloud environments.
	  ◦ **CipherTrust Application Data Protection** delivers key management, signing, and encryption services enabling comprehensive protection of files.
	  ◦ **CiphterTrust Manager** centrally manages encryption keys and configures security policies so organizations can control and protect sensitive data with the separation of duties.
	
	Protect Sensitive Data in Motion
	
	• **Thales High Speed Encryptors (HSEs)** provide network independent data-in-transit/ motion encryption (Layers 2,3 and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. It allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception— without performance compromise.

INCIDENT MANAGEMENT – DETECTION OF SECURITY COMPROMISES	
Guidelines 69 APRA envisages that a regulated entity would establish a clear **allocation of responsibilities for monitoring processes**, with appropriate tools in place to enable timely detection. **Access controls and segregation of duties** would typically be used as a means to safeguard the integrity of the monitoring processes.	• With the **CipherTrust Data Security Platform**, administrators can create **strong separation of duties between privileged administrators and data owners**. Strong separation of duties policies can be enforced to ensure one administrator does not have complete control over data security activities, encryption keys, or administration. In addition, the **CipherTrust Manager** supports two-factor authentication for administrative access. • **Thales OneWelcome Identity Platform** allows organizations to virtually (or logically) limit access to confidential resources through the use of MFA (including phishing-resistant authentication) and granular access policies. The platform tracks identity events and provides analytics reports, including failed login attempts, user profile changes, changes to credentials and devices, consent grants and revocations, changes to group memberships, etc.
Attachment A: Security Principles 1. (a) Implement **multiple layers and types of controls** such that if one control fails, other controls limit the impact of an information security compromise. This is typically referred as the principle of 'defence in depth'	• **CipherTrust Manager** offers centralized Administration and Access Control, which unifies key management operations with role-based access controls. • **Hardware security modules (HSMs)** safeguard the cryptographic keys used to secure applications and sensitive data, it further enhances security and ensures compliance with an additional layer of protection.

Prudential Practice Guidelines (PPG) for CPS234	Thales Solution

Attachment A: Security Principles 1. (e)
 	
Use of, and access to, information assets is attributable to an individual, hardware or software, and **activity logged and monitored**
	• **Thales OneWelcome** Identity platform allows organizations to
	  ◦ identify and authenticate internal and external users, so organizations can limit the access to confidential resources through use of MFA and granular access policies. Its fine-grained authorization capability based on user entity attributes helps organizations by providing the right amount of access to the right people at the right time.
	  ◦ manage the third party identity efficiently with its' delegation management capability and to mitigate risks from third party.
	  ◦ respond and mitigate risks by providing an immediate and an 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.
	• After user is identified, you can control and coordinate how users gain access to assets, and what they can do with those assets with **CipherTrust Enterprise Key Management Solution**. It streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases with robust Auditing and reporting.

Attachment C: Identity and Access	• **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.
Attachment E: Cryptographic Techniques	• **Luna HSMs** from Thales provide a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Available in three FIPS 140-2 certified form factors, **Luna HSMs** support a variety of deployment scenarios. • **CipherTrust Data Security Platform** can enforce very granular, least-privileged-user access management policies, enabling protection of data from misuse by privileged users and APT attacks.

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.