Compliance Brief

THALES

CYBERSECURITY

Addressing the APRA Prudential Practice Guideline for CPS234 Compliance in Australia

cpl.thalesgroup.com

THALES

CYBERSECURITY

What is APRA Prudential Practice Guideline (PPG)?
The purpose of Prudential Practice Guidelines (PPG) CPG234 Information Security 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

How Thales Helps with CPS234 Compliance

Thales helps regulated entities comply with CPS234 by addressing the 5 guidance areas of the Prudential Practice Guidelines (PPG) CPG234: Information Security Capability, Policy Framework, Information Asset Identification and Classification, Implementation of Controls, and Incident Management.

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.

CPS234 Requirement	PPG234 Section	How Thales Helps
Information Security Capability	17 & 18	Data Security, IAM
Policy Framework	21a – e, g, k & Attachment C	Application Security, Data Security, IAM
Information Asset Identification and Classification	27, 29 & 30	Data Security
Implementation of Controls		
• Information security controls implemented at all stages	36a – e & m; 39a & d	Application Security, Data Security, IAM
• Minimise Exposure to Plausible Worst Case Scenarios	44	
• Security in Change Management	47a	Data Security, IAM
• Software Security	48	Application Security, Data Security
• Cryptographic Techniques to Restrict Access	54, Attachment E	Data Security
• Information Security Technology Solutions	56	Data Security, IAM
• End-User Developed/ Configured Software	58	Data Security
Incident Management	69	Data Security, IAM
Attachment A	1a & 1e	

PPG234 – Guidance	How Thales Helps	Solution Areas
INFORMATION SECURITY CAPABILITY – Capability of Third Parties and Related Parties		
17. APRA-regulated entities often place reliance on **information security capabilities of third parties** and related parties to provide a targeted information security capability, or as part of a wider service-provision arrangement. 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.	• Provide **data activity monitoring** for structured and unstructured data across cloud and on-prem systems. • **Enforce separation of duty** between your data and external parties as well as your cloud service provider **(CSP)** by securely storing encryption keys outside of the corresponding cloud. • Offer advanced multi-cloud **Bring Your Own Encryption (BYOE)** solutions to ensure data mobility to efficiently secure data across multiple cloud vendors with centralized and independent encryption key management. • **Centralize key lifecycle management**, including generation, rotation, destruction, import, and export. • Enforce **access controls**, including the use of passphrases or key encryption keys. Private keys stored in the HSM remain encrypted and require proper authentication to access. • Enable **relationship management** with suppliers, partners or any third-party user; with clear delegation of access rights. • **Minimize privileges** by using relationship-based fine-grained authorisation. • **Manage all users**, including the workforce, contractors, third-party users such as customers, suppliers, logistics, and B2B or B2C type users.	**Data Security** Cloud Key Management Data Activity Monitoring Data Discovery & Classification Data Risk Analytics Hardware Security Modules High-Speed Encryption Key Management Secrets Management Tokenization Transparent Encryption **Identity & Access Management** Delegated User Management Third-party Access Control Thales OneWelcome Identity Platform
POLICY FRAMEWORK – A Policy Hierarchy Informed by a Set of Key Principles		
21. (a) **identification, authorisation and granting** of access to information assets (refer to Attachment C for further guidance) **Attachment C**	• Limit access to systems and data based on **roles and context** with policies. • Apply **contextual security measures** based on risk scoring. • Enable **continuous monitoring** to capture and analyze all data store activity, providing **detailed audit trails** that show who access what data, when, and what was done to the data. • Enable the **separation of duties** between the security administrator and the system administrator inside servers, ensuring the system admins or privileged accounts do not have access to sensitive encryption keys, while the security administrators do not have access to the data. • Centralize **access policies and enforcement** across multiple hybrid environments in a single pane of glass. • Offer "**least privilege**" access rights where minimum sufficient permissions are granted to legitimate users and adhere to a "**deny all**" access control policy for users by default. • Deploy **time-bound access** that restricts access to a specific period based on the nature of work. • Adopt robust **user authorisation and authentication** based on the criticality of IT assets by defining the right access policies, step-up authentication, and enforcing phishing-resistant authenticators. • Manage authentication and access control by supporting **Multi-Factor Authentication** and Single Sign-On (**SSO**) and displaying access log reports.	**Data Security** Data Activity Monitoring Data Risk Analytics Transparent Encryption **Identity & Access Management** Authentication Service – Private Cloud Multi-Factor Authentication SafeNet Trusted Access (STA) Single Sign-On (SSO) Workforce Access Management

PPG234 – Guidance	How Thales Helps	Solution Areas
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**	• **Classify and assign specific sensitivity levels** for data when you are defining your data stores and your classification profiles for different types of data sets. • Identify the current state of **compliance and document gaps**. • **Encrypt data at rest** on-premises, across clouds, and in big data or container environments. • **Pseudonymize sensitive data** at the source, ensuring that cleartext data is never exposed to unauthorized applications or personnel during processing or storage. • Offer advanced multi-cloud **Bring Your Own Encryption (BYOE)** solutions to ensure data mobility to efficiently secure data across multiple cloud vendors with centralized and independent encryption key management. • Provide **data activity monitoring** for structured and unstructured data across cloud and on-prem systems. • Ensure **secure deletion** by removing keys from CipherTrust Manager, digitally shredding all instances of the data. • Enforce **access controls**, including the use of passphrases or key encryption keys. Private keys stored in the HSM remain encrypted and require proper authentication to access. • **Protect data in use** by leveraging confidential computing. • Enable **relationship management** with suppliers, partners or any third-party user; with clear delegation of access rights. • **Minimize privileges** by using relationship-based fine-grained authorisation.	**Data Security** Data Activity Monitoring Data Discovery & Classification Data Risk Analytics Hardware Security Modules Key Management Secrets Management Transparent Encryption Tokenization **Identity & Access Management** Delegated User Management Third-party Access Control
21. (c) **Management of information security technology** solutions that include **firewall**, anti-malicious software, intrusion detection/ prevention, cryptographic systems and monitoring/ log analysis tools	• Offer a highly **available and distributed security architecture** that eliminates single points of failure and protects critical systems from network faults and cyber threats, and supports reliable network service delivery. • **Safeguard** critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic. • Offer a guaranteed **SLA of 3 seconds or less** for DDoS attacks targeting Layers 3 and 4, and protect organisations against volumetric and protocol-based threats. • **Block threats** such as SQL injection, XSS, and other OWASP Top 10 vulnerabilities – safeguarding web applications from threats. Offer **proactive managed rules** to ensure organisations have the most up-to-date protection against common attack vector threats. • **Centralize key lifecycle management** tasks including generation, rotation, destruction, import and export. • **Protect cryptographic keys** in a tamper-resistant FIPS 140-3 Level 3 validated environment for securing the key lifecycle. • Manage and protect all **secrets and sensitive credentials**. • Offer **key rotation** that can assist in case of recovery where cryptographic keys are compromised. Keys can be rotated on demand to minimize the impact of any key compromises.	**API Protection** API Security DDoS Protection Web Application Firewall **Data Security** Hardware Security Modules High-Speed Encryption Key Management Secrets Management Transparent Encryption

PPG234 – Guidance	How Thales Helps	Solution Areas
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** 21. (e) **monitoring** and incident management to address the identification and classification of incidents, reporting and escalation guidelines, preservation of evidence and the investigation process; 21. (g) **acceptable usage of information assets** that define the information security responsibilities of end-users including staff, third parties, related parties and customers (refer to Attachment B and Attachment F for further guidance);	• Limit access to systems and data based on **roles and context** with policies. • Apply **contextual security measures** based on risk scoring. • Enable **continuous monitoring** to capture and analyze all data store activity, providing **detailed audit trails** that show who accesses what data, when, and what was done to the data. • Centralize **access policies and enforcement** to multiple hybrid environments in a single pane of glass. • Provide a **unified strategy** for access control across all user populations. • Enable a consistent and **policy-driven approach** to identification, authentication, and authorisation of all users to their IT assets, data, and services. • **Manage all users**, including the workforce, contractors, third-party users such as customers, suppliers, logistics, and B2B or B2C type users. • Offer "**least privilege**" access rights where minimum sufficient permissions are granted to legitimate users and adhere to a "**deny all**" access control policy for users by default.	**Data Security** Data Activity Monitoring Data Risk Analytics Transparent Encryption **Identity & Access Management** Identity Verification Multi-Factor Authentication Thales OneWelcome Identity Platform Workforce Access Management
21. (k) mechanisms to **assess compliance** with, and the ongoing effectiveness of, the **information security policy framework**	• Enable **continuous monitoring** to capture and analyze all data store activity, providing **detailed audit trails** that show who accessed what data, when, and what was done to the data. • Support the **creation of audit trail reports** of all access for auditing and investigation in the event of any incidents. • Produce an auditable trail of permitted and denied access attempts with Security Intelligence to streamline compliance reporting and **speed up threat detection** using leading SIEM systems.	**Data Security** Data Activity Monitoring Data Risk Analytics Security Intelligence Transparent Encryption

PPG234 – Guidance	How Thales Helps	Solution Areas
INFORMATION ASSET IDENTIFICATION AND CLASSIFICATION – Classification of all information assets by criticality and sensitivity		
27. Under CPS 234, all information assets must be **classified by criticality and sensitivity. Classification methodology** 29. In order to identify and classify information assets, an APRA-regulated entity would benefit from maintaining a **classification methodology** that provides clarity as to what constitutes an information asset, granularity considerations and the method for rating criticality and sensitivity. 30. APRA-regulated entities record information assets in various ways, sometimes at a very **granular level** and sometimes at an aggregated level.	• **Classify and assign specific sensitivity levels** for data when you are defining your data stores and your classification profiles for different types of data sets. • Enable **continuous monitoring** to capture and analyze all data store activity, providing **detailed audit trails** that show who accesses what data, when, and what was done to the data. • Enforce **granular access control** (separated from the OS access control) with transparent encryption for privileged users to prevent misuse or abuse.	**Data Security** Data Activity Monitoring Data Discovery & Classification Data Risk Analytics Key Management Transparent Encryption
36. (b) **configuration management** – the configuration of information assets **minimises vulnerabilities** and is defined, assessed, registered, maintained, including when new vulnerabilities and threats are discovered, and applied consistently;	• Offer **advanced API Verification capabilities** to strengthen your defenses against potential vulnerabilities. • Run **assessment tests** on data stores such as MySQL or so to scan for known vulnerabilities. • **Scan your databases** with over 1,500 predefined vulnerability tests based on CIS and PCI-DSS benchmarks to help you keep your databases covered for the latest threats.	**Application Security** API Protection **Data Security** Data Activity Monitoring
36. (c) **Deployment and Environment Management** – development, test and production environments are appropriately **segregated and enforce separation of duties**	• Manage **encryption keys** and **configure security policies** centrally, enabling organisations to control and protect sensitive data through separation of duties. • Offer **transparent encryption** and access control for data residing. • **Encrypt sensitive data** once it is created and make sure cleartext data will not be processed or stored by unauthorized applications and personnel. • Allow root users to do their job without abusing data by **privileged user access controls**. • Enforce granular **privileged-user-access management** policies that can be applied by user, process, file type, time of day, and other parameters. • Provide complete **separation of roles** where only authorized users and processes can view unencrypted data.	**Data Security** Key Management Tokenization Transparent Encryption

PPG234 – Guidance	How Thales Helps	Solution Areas
36. (d) **Access Management Controls** – only **authorised users are able to access** information assets (refer to Attachment B for further guidance)	• Manage encryption keys, provide **granular access control** and configure security policies. • Enforce **granular access control** (separated from the OS access control) with transparent encryption for privileged users to prevent misuse or abuse. • **Manage system and data access rights** (access control) by supporting role-based authorisation (**Role-Based Access Control (RBAC)**) and conditional authorisation (**ABAC**). • Control and manage **privileged user accounts** with granular access policies, and fine-grained authorisation policies by supporting the enforcement of multi-factor authentication (MFA) for accessing critical systems. • Design authorisation and approval procedures (User Journey Orchestration) **for privileged user accounts** and store and display as a privileged user activity report for detailed auditing. • Limit the access of internal and external users based on their **roles and context** with Identity Platform. • Implement physical access to sensitive facilities with **SafeNet IDPrime smart cards**, which can also augment Passwordless authentication initiatives relying on PKI and FIDO technology.	**Identity & Access Management** Adaptive Access Control Delegated User Management Multi-Factor Authentication Risk-Based Authentication Thales OneWelcome Identity Platform User Journey Orchestration
36. (e) **Hardware and software asset controls – appropriate authorisation** to prevent security compromises from unauthorised hardware and software assets	• Employ **digital Signing** for a wide range of applications with **Hardware security modules (HSMs)** to protect the private keys used for secure electronic signatures. • Support B2B and third-party i**dentity access management** for connected devices and external parties. • Provides **authorisation** and **access-control policies** that can be used to govern access from external, browserless, or constrained devices where integrated.	**Data Security** Hardware Security Modules **Identity & Access Management** Thales OneWelcome Identity Platform
36. (m) **Service provider and Management Controls** – to ensure that a regulated entity's **information security requirements** are met.	• Provide **data activity monitoring** for structured and unstructured data across cloud and on-prem systems. • Monitor **data access activity** over time to set up alerts on activity that can put organisations at risk. • Offer advanced multi-cloud **Bring Your Own Encryption (BYOE)** solutions to ensure data mobility to efficiently secure data across multiple cloud vendors with centralized and independent encryption key management. • **Retain full control and ownership** of the sensitive data by controlling access to encryption keys via Cloud Key Management, negating the risk of data being released to foreign powers with the **Hold-Your-Own-Key (HYOK**) approach. • Enforce **access controls**, including the use of passphrases or key encryption keys. Private keys stored in the HSM remain encrypted and require proper authentication to access. • Enable **relationship management** with suppliers, partners or any third-party user; with clear delegation of access rights. • **Minimize privileges** by using relationship-based fine-grained authorisation. • **Manage all users**, including the workforce, contractors, third-party users such as customers, suppliers, logistics, and B2B or B2C type users.	**Data Security** Cloud Key Management Data Activity Monitoring Data Discovery & Classification Data Risk Analytics Hardware Security Modules High-Speed Encryption Key Management Secrets Management Tokenization Transparent Encryption **Identity & Access Management** Delegated User Management SafeNet Trusted Access Thales OneWelcome Identity Platform

PPG234 – Guidance	How Thales Helps	Solution Areas
39. **Vulnerabilities and threats are identified, assessed and remediated** a. implement mechanisms that access and analyse timely threat intelligence regarding vulnerabilities, threats, methods of attack and countermeasures; d. implement mechanisms to **disrupt the various phases of an attack**. Example phases include reconnaissance, vulnerability exploitation, malware installation, privilege escalation, and unauthorised access.	• **Detect system threats** with Web Application Firewall, API Security and Database Security and stream logs to SIEM system. • **Monitor API activity**, track usage, detect anomalies, and identify potential unauthorized access attempts. • Offer **advanced API Verification capabilities** to strengthen your defenses against potential vulnerabilities. • **Safeguard** critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic. • Run **assessment tests** on data stores such as MySQL or so to scan for known vulnerabilities. • **Scan your databases** with over 1,500 predefined vulnerability tests based on CIS and PCI-DSS benchmarks to help you keep your databases covered for the latest threats. • Eliminate the **threat of an unauthorized or compromised user account** gaining stealthy access to sensitive data with Security Intelligence logs that produce an auditable trail of permitted and denied access attempts from users and processes. • Monitor 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. • Adjust **access permissions** based on real-time or near **real-time user behavior** and contextual factors, and maintain the highest level of security. • **Monitor user behavior** such as admin login from a new location/IP or a wrong system access pattern to alert and prevent attacks.	**Application Security** API Protection Attack Analytics Bot Protection DDoS Protection Web Application Firewall **Data Security** Data Activity Monitoring File Activity Monitoring Security Intelligence Transparent Encryption Ransomware Protection **Identity & Access Management** Adaptive Access Control

PPG234 – Guidance	How Thales Helps	Solution Areas
IMPLEMENTATION OF CONTROLS – Minimise Exposure to Plausible Worst Case Scenarios		
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.	• Enforce very **granular** and **least-privileged-user access management** policies, enabling protection of data from misuse by privileged users and APT attacks. • **Encrypt files**, while leaving their metadata in the clear, so 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. • **Encrypt sensitive data** once it is created and make sure cleartext data will not be processed or stored by unauthorized applications and personnel. • Monitor 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. • Safeguard the **cryptographic keys** used to secure applications and sensitive data with HSMs. • Offer **centralized Administration and Access Control** with role-based access controls. Using existing AD and LDAP credentials to authenticate and authorize administrators and key users, and prevent unauthorized password changes and alerts on simultaneous logins by the same user. • Offer **key rotation** that can assist in case of recovery where cryptographic keys are compromised. Keys can be rotated on demand to minimize the impact of any key compromises.	**Data Security** Data Activity Monitoring Hardware Security Modules Key Management Tokenization Transparent Encryption Ransomware Protection **Identity & Access Management** Adaptive Access Control Delegated User Management Fraud and Risk Management Workforce Access Management
IMPLEMENTATION OF CONTROLS – Security in Change Management		
47. APRA envisages that a regulated entity would implement **controls to manage changes** to information assets, including changes to hardware, software, data, and configuration (both where the change is planned and in response to an emergency)	• Centrally **enforce key rotation** policies by automating rotation schedules, propagating new key versions, automatically rekeying protected data, and providing role-based access control with full audit logging. • Provide **role-based access control (RBAC)** to keys and policies, ensuring only authorized administrators can define or change rotation policies. • Ensure only authorized users can **grant** or **change access rights**; enforce consistent authorization policies across environments.	**Data Security** Key Management Secrets Management **Identity & Access Management** Adaptive Access Control SafeNet Trusted Access Thales OneWelcome Identity Platform

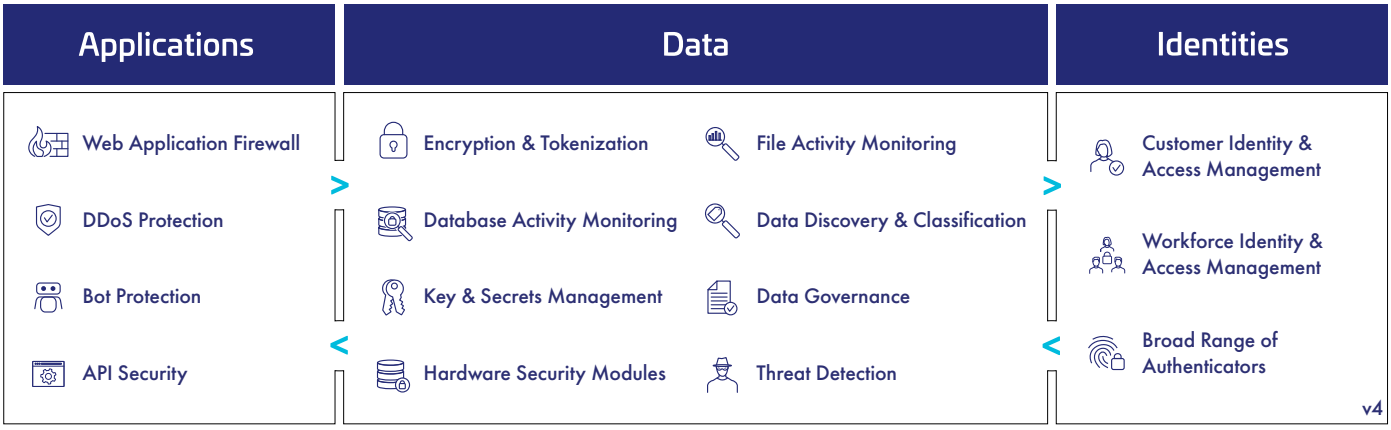
PPG234 – Guidance	How Thales Helps	Solution Areas
IMPLEMENTATION OF CONTROLS – SOFTWARE SECURITY		
48. An APRA-regulated entity would typically implement **secure software development** and acquisition techniques to assist in maintaining confidentiality, integrity and availability by improving the general quality and vulnerability profile of the software (refer to Attachment D for further guidance).	• 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. • **Encrypt sensitive data** once it is created and make sure cleartext data will not be processed or stored by unauthorized applications. • Enforce **security-by-design** by ensuring sensitive data is protected during system development and modification. • Provide developers with **accessible data protection tools** such as encryption and key management to integrate security early in the development lifecycle and foster DevSecOps practices. • Shift Data Security operations to Data Security Admins, enabling **better segregation of duties** and change control for system modifications. • **Deploy data protection controls** in hybrid and multi-cloud applications to protect DevSecOps. • Easily access data security solutions through **online marketplaces**. • Protect and automate access to **secrets** across DevOps tools. • Secure **change management** by enabling integration tools for versioning, traceability, and rollback capabilities. • Safeguard critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic. • Detect and prevent cyber threats with **web application firewall**, ensuring seamless operations and peace of mind.	**Application Security** API Protection Bot Protection DDoS Protection Web Application Firewall **Data Security** Application Data Protection Community Edition Data Protection Gateway DPOD Marketplace High-Speed Encryption Key Management RESTful Data Protection Secrets Management Tokenization
IMPLEMENTATION OF CONTROLS – Cryptographic Techniques to Restrict Access		
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). **Attachment E**	• Provide **various encryption options** and methods to protect their data stored. • **Centralize key lifecycle management** tasks including generation, rotation, destruction, import and export. • **Protect the root-of-trust** of a cryptographic system within FIPS140-2 Level 3 - a highly secure environment. • Provide strong access controls to prevent unauthorized users from accessing **sensitive cryptographic material**. • Employ a **three-layer authentication model** to control administrative, client, and application access for data stored on the cryptographic engine. • Secure **data in transit** as it moves from site-to-site, or from on-premises to the cloud and back at Layers 2, 3, and/or 4 without slowing down the network.	**Data Security** Hardware Security Modules High-Speed Encryption Key Management Tokenization Transparent Encryption

PPG234 – Guidance	How Thales Helps	Solution Areas
IMPLEMENTATION OF CONTROLS – Information Security Technology Solutions		
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**	• Manage **encryption keys** centrally, provide granular access control, and configure security policies. • Enforce **access controls**, including the use of passphrases or key encryption keys. Private keys stored in the HSM remain encrypted and require proper authentication to access. • **Pseudonymize sensitive data** at the source, ensuring that cleartext data is never exposed to unauthorized applications or personnel during processing or storage. • **Record access** to the database system and detect login attempts on the database system. • Detect and alert administrators if **abnormal access attempts** are found, and administrators can respond quickly. • Detect and pinpoint **critical threats to data**, prioritizes what matters most, and provides actionable insights. • Support the **creation of audit trail reports** of all accesses for auditing and investigation in the event of any incidents. • Offer 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.	**Data Security** Application Data Protection Data Activity Monitoring Data Risk Analytics Enterprise & Cloud Key Management Hardware Security Modules **Identity & Access Management** Delegated User Management Third-party Access Control
IMPLEMENTATION OF CONTROLS – End-User Developed/ Configured Software		
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.	• Protects data with **data-at-rest encryption**, access controls, and data access audit logging. • Deliver capabilities for database **tokenization** and dynamic display security and secures pseudonymizing sensitive assets. • Manage **encryption keys** and configure security policies to control and protect sensitive data with the separation of duties.	**Data Security** Key Management Secrets Management Tokenization Transparent Encryption

PPG234 – Guidance	How Thales Helps	Solution Areas
INCIDENT MANAGEMENT – Detection of Security Compromises		
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.	• Create **strong separation of duties** between privileged administrators and data owners to ensure one administrator does not have complete control over data security activities, encryption keys, or administration. • Support **two-factor authentication** for administrative access for centralized key management. • Allow organizations to virtually (or logically) limit access to confidential resources with **MFA** (including phishing-resistant authentication) and **granular access policies**. • Track **identity events** and provide **analytics reports**, including failed login attempts, user profile changes, changes to credentials and devices, consent grants and revocations, changes to group memberships.	**Data Security** Key Management Secrets Management Tokenization Transparent Encryption **Identity & Access Management** Adaptive Access Control Delegated User Management Multi-Factor Authentication Risk-Based Authentication Thales OneWelcome Identity Platform User Journey Orchestration
Attachment A		
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.'	• Offer **centralized Administration and Access Control**, which unifies key management operations with role-based access controls. • Secure applications and sensitive data with HSM to ensure compliance with an **additional layer of protection**.	**Data Security** Hardware Security Modules Key Management
1. (e) Use of, and access to, information assets is attributable to an individual, hardware or software, and **activity logged and monitored**	• **Identify and authenticate** internal and external users to limit access to confidential resources with MFA and granular access policies. • Manage the third-party identity efficiently with its **delegation management** capability and mitigate risks from third parties. • Provide an immediate and up-to-date **audit trail of all access events** to all systems and stream logs to external SIEM systems. • Streamline and strengthen **key management** in cloud and enterprise environments over a diverse set of use cases with robust **auditing and reporting**.	**Data Security** Key Management Secrets Management **Identity & Access Management** Adaptive Access Control Delegated User Management Multi-Factor Authentication Thales OneWelcome Identity Platform

Thales provides comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

Security for What Matters Most



Application Security: Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs and a secure Content Delivery Network (CDN).

Data Security: Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.

Identity & Access Management: Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

Organizations can leverage Thales' suite of identity, application and data security solutions available on a single unified platform to become compliant today and stay compliant in the future. Contact us now!

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.