White Paper

THALES
CYBERSECURITY

Complying with the MAS TRM Guidelines in Singapore

cpl.thalesgroup.com

THALES

CYBERSECURITY

The Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines was introduced in 2001 and revised in January 2021, provide a framework of best practices for Financial Institutions (FIs) in Singapore to identify, assess, and manage technology and cyber risks, ensuring the security, reliability, and resiliency of their systems.

Purpose

The MAS TRM guidelines aim to help FIs proactively manage technology-related risks, safeguard against sophisticated cyber threats, ensure operational continuity, and maintain the integrity of Singapore's financial sector. The 2021 update strengthened the focus on cyber threats and on senior management's accountability for ensuring robust technology risk controls.

- **Strengthening Cyber Resilience:** Providing a framework to detect, prevent, and respond to rising cyber threats.
- **Ensuring System Reliability:** Establishing standards for high availability, recovery, and security of critical IT infrastructure.
- **Improving Risk Governance:** Setting expectations for oversight, including managing third-party and vendor risks.
- **Addressing New Technologies:** Covering risks related to cloud computing, virtualization, and the Internet of Things (IoT).

Scope

The TRM Guidelines apply to all FIs regulated by MAS, including, but not limited to:

- Banks (local and foreign, wholesale, and merchant).
- Insurance companies and intermediaries.
- Capital Markets Services (CMS) Licensees (fund managers, brokers).
- Payment Service Providers and Fintechs (including digital token providers).

The key requirements are as follows:

- **Risk Governance:** Board and senior management oversight, risk appetite, and accountability.
- **Cybersecurity Controls:** Network security, access controls, malware protection, and data loss prevention.
- **Third-Party Management:** Vetting vendors, conducting due diligence, and managing concentration risks.
- **Operational Resilience:** System availability, disaster recovery, and business continuity planning.
- **Systems Development:** Secure coding, software development lifecycle (SDLC), and security testing.

How Thales Helps with the MAS TRM Guidelines?

Thales' solutions can help Financial Institutions (FIs) in Singapore address the TRM Guidelines across 11 key requirements by simplifying compliance and automating security with visibility and control, thereby reducing the burden on security and compliance teams.

Guidelines	How Thales Helps	Solution Areas
4. Technology Risk Management Framework		
4.1 – Risk Management Framework **4.1.2:** "... achieve data confidentiality **and integrity, system security and reliability**, as well as stability and resilience in its IT operating environment..." **4.1.4:** "... should also encompass the following components..." • risk identification • risk assessment • risk treatment • risk monitoring, review and reporting	• **Manage encryption keys** centrally, provide granular access control, and configure security policies. • **Protect cryptographic keys** in a tamper-resistant FIPS 140-3 Level 3 validated environment for securing the key lifecycle. • **Detect and pinpoint critical threats** to data, prioritize what matters most, and provide actionable insights to accelerate threat investigation and response.	**Data Security** • Data Risk Analytics • Key Management • Hardware Security Modules

Guidelines	How Thales Helps	Solution Areas
4.2 – Risk Identification **4.2.1:** "... identify the **threats and vulnerabilities** applicable to its IT environment, including **information assets** that are maintained or supported by **third party service** providers..."	• 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 FIs 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. • **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. • **Enforce separation of duty** between your data and external party as well as your cloud service provider (CSP) by securely storing encryption keys outside of the corresponding cloud.	**Data Security** • Data Activity Monitoring • Data Discovery & Classification • Data Risk Analytics • High-Speed Encryption • Hardware Security Modules • Cloud Key Management • Key Management • Secrets Management • Tokenization • Transparent Encryption
4.3 – Risk Assessment **4.3.1:** "... perform an analysis of the potential impact and consequences of the **threats and vulnerabilities** on the overall business and operations... should take into consideration financial, operational, legal, reputational and regulatory factors in assessing technology risks..." **4.3.2: " ... prioritisation of technology risks,** a set of criteria measuring and determining the likelihood and impact of the risk scenarios ..."	• 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. • Detect and virtually **patch database software vulnerabilities.**	**Data Security** • Data Activity Monitoring
4.4.5 Risk Monitoring, Review and Reporting **4.5.1:** "...institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks..." **4.5.3:** "... technology risk metrics should be developed to **highlight information assets** that have the highest risk exposure... take into account risk events and audit observations, as well as applicable regulatory requirements..."	• **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.	**Data Security** • Data Activity Monitoring • Data Discovery & Classification • Data Risk Analytics

Guidelines	How Thales Helps	Solution Areas
6. Software Application Development and Management		
6.3 – DevSecOps Management **6.3.1:** "... automating and integrating IT operations, quality assurance and **security practices in the software development process...** ensure its DevSecOps activities and processes are aligned with its SDLC framework and IT service management processes (e.g. configuration management, change management, software release management). **6.3.2:** "... implement adequate security measures and **enforce segregation of duties** for the software development, testing and release functions in its DevSecOps processes..."	• 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.	**Application Security** • Account Takeover Protection • API Security • Attack Analytics • Bot Protection • DDoS Protection • Web Application Firewall **Data Security** • Community Edition • Hardware Security Modules • Secrets Management
6.4 – Application Programming Interface Development **6.4.3:** "... perform a **risk assessment** before allowing third parties to connect to its **IT systems via APIs,** and ensure the implementation for each API is commensurate with the **sensitivity and business criticality of the data** being exchanged, and the confidentiality and integrity requirements of the data. **6.4.4: "...Security standards** for designing and developing **secure APIs** should be established... include the measures to **protect the API keys or access tokens**... A reasonable timeframe should be defined and enforced for access token expiry to reduce the risk of unauthorised access..." **6.4.5: "...Strong encryption standards and key management** controls ... to **secure transmission** of sensitive data through **APIs**..."	• Provide continuous **discovery and classification** potential risk of all public, private, and shadow APIs. • **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 your login endpoints from credential stuffing, **brute force attacks**, and **account fraud**. • Detect and prevent cyber threats with **web application firewall**, ensuring seamless operations and peace of mind. • Enable **complete visibility** and help in **singling out enterprise-wide attack campaigns**.	**Application Security** • Application Security • Account Takeover Protection • API Security • Attack Analytics • Bot Protection • DDoS Protection • Web Application Firewall **Data Security** • Data Security • Community Edition • Hardware Security Modules • Secrets Management

Guidelines	How Thales Helps	Solution Areas
6.4.7: "...Detective measures, such as technologies that **provide real-time monitoring and alerting** ... to provide visibility of the usage and performance of **APIs**, and detect suspicious activities... established to promptly **revoke the API keys** or access token in the event of a breach..." **6.4.8:** "... ensure adequate system capacity is in place to handle **high volumes of API cal**l requests, and implement measures to mitigate cyber threats such as **denial of service (DoS) attacks**..."	• Safeguard critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic. • Protect against both **volumetric and application-layer DDoS attacks** in one scalable solution at ease. • Deploy **data protection controls** in hybrid and multi-cloud applications to protect DevSecOps. • Protect and automate **access to secrets** across DevOps tools. • Enable **comprehensive secrets management** of credentials, certificates and keys, including static secrets, dynamic secrets, SSH keys, API keys and tokens. • Offer FIPS 140-2 Level 3 **root of trust** for credentials and keys..	
7. IT Service Management		
7.4 – Patch Management **7.4.1:** "... ensure applicable functional and non-functional **patches** (e.g. fixes for **security vulnerabilities** and software bugs) are implemented ... commensurate with the criticality of the patches and the FI's IT systems..." **7.4.2:** "...Patches **should be tested** ... in the production environment to **ensure compatibility** with existing IT systems or they do not introduce problems to the IT environment..."	• 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. • Detect and virtually **patch database software vulnerabilities.**	**Data Security** • Data Activity Monitoring
8. IT Resilience		
8.5 – Data Centre Resilience **8.5.6:** "...The DC should have adequate **physical access controls**..."	• Leverage **smart cards** for implementing physical access to sensitive facilities. • **Limit access** to systems and data based on roles and context with policies.	**Identity & Access Management** • Smart cards
9. Access Control		
9.1 – User Access Management **9.1.1:** "...The principles of **'never alone', 'segregation of duties', and 'least privilege'** should be applied ... no one person has access to perform sensitive system functions..."	• Limit access to systems and data based on **roles and context** with policies. • Apply **contextual security measures** based on risk scoring.	**Data Security** • Data Activity Monitoring • Data Risk Analytics • Transparent Encryption

Guidelines	How Thales Helps	Solution Areas
9.1.2: "... establish a **user access management** process to provision, change and revoke access rights to information assets. Access rights should be authorised and approved by appropriate parties..." **9.1.3:** "... ensure **records of user access and user management** activities are uniquely identified and **logged for audit** and investigation purposes..." **9.1.5: "...Multi-factor authentication** should be implemented ... access to sensitive system functions to safeguard the systems and data from unauthorised access..." **9.1.7:** "...granted access rights on a **need-to-use basis..."**	• 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. • 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** to 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** which restricts access to a specific period based on the nature of work. • Adopt robust **user authorization 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.	**Identity & Access Management** • Authentication Service – Private Cloud • Multi-Factor Authentication • SafeNet Trusted Access (STA) • Single Sign-On (SSO) • Workforce Access Management
9.2 – Privileged Access Management **9.2.1:** "... Access to **privileged accounts** should only be granted on **a need-to-use basis;** activities of these accounts should be logged and reviewed as part of the FI's **ongoing monitoring..."** **9.2.2: "...establish a process to manage and monitor the use of system and service accounts for suspicious or unauthorised activities..."**	• 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 authorization (**RBAC**) and conditional authorization (**ABAC**). • Control and manage **privileged user accounts** by supporting the enforcement of multi-factor authentication (MFA) for accessing critical systems. • Design authorization and approval procedures (User Journey Orchestration) **for privileged user accounts** and store and display as a privileged user activity report for detailed auditing.	**Data Security** • Transparent Encryption **Identity & Access Management** • Adaptive Access Control • Delegated User Management • Multi-Factor Authentication • Risk-Based Authentication • User Journey Orchestration

Guidelines	How Thales Helps	Solution Areas
9.3 – Remote Access Management **9.3.1: "... Remote connections should be encrypted ... Strong authentication,** such as multi-factor authentication, should be **implemented** for users performing remote access to safeguard against unauthorised access ..." **9.3.2:** "... ensure remote access to the FI's information assets is only **allowed from devices that have been secured** according to the FI's security standards..."	• Enable **secure remote access** for employees to all company resources on-premises or in the cloud with a seamless user experience. • Enable MFA with the **broadest range** of hardware and software methods. • Build and deploy **adaptive authentication** policies. • Offer **Remote Access Policies** to control only pre-approved users. • Store **Remote Access Logs** to support retrospective auditing. • **Encrypt data sent over remote connections** (Data-in-Transit Encryption) to prevent data interception during communication.	**Identity & Access Management** • Adaptive Access Control • Fraud & Risk Management • Multi-Factor Authentication • Risk-Based Authentication • Workforce Access Management
10. Cryptography		
10.1 – Cryptographic Algorithm and Protocol **10.1.2:** "... adopt **cryptographic** algorithms from well-established **international standards..."** **10.1.4:** "... ensure all **cryptographic algorithms** used have been subject to **rigorous testing or vetting** to meet the identified security objectives and requirements..."	• Offer **leading cryptographic solutions** that are rigorously tested, validated, and compliant with internationally recognized standards, such as FIPS 140-3 and **Common Criteria** Certifications. • Support algorithms such as AES, SHA-2 family, ECDH, RSA, and ECDSA, ensuring the use of **strong and approved algorithms** in cryptographic operations. • Offer native support to **NIST-Standardized PQC Algorithms:** ML-KEM (FIPS 203) and ML-DSA (FIPS 204).	**Data Security** • Key Management • Hardware Security Modules
10.2 – Cryptographic Key Management **10.2.1:** "...Cryptographic **key management policy, standards and procedures** covering key generation, distribution, installation, renewal, revocation, recovery and expiry should be established..." **10.2.2:** "... ensure cryptographic keys are **securely generated and protected** from unauthorised disclosure. Any cryptographic key or sensitive data used to generate or derive the keys should be also be **protected or securely destroyed..."**	• **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. • **Automate key lifecycle management** across clouds and hybrid environments with processes and tools. • Manage and protect all **secrets and sensitive credentials.** • **Protect cryptographic keys** in a FIPS 140-3 Level 3 environment. • Ensure **secure deletion** by removing keys from CipherTrust Manager, digitally shredding all instances of the data.	**Data Security** • Hardware Security Modules • High-Speed Encryption • Key Management • Secrets Management • Tokenization • Transparent Encryption

Guidelines	How Thales Helps	Solution Areas
10.2.3: "... determine the appropriate **lifespan of each cryptographic key** based on factors ... The cryptographic key should be **securely replaced**, before it expires at the end of its lifespan..." **10.2.4:** "... protect sensitive cryptographic keys... manage, process and store such keys in hardened and tamper resistant systems, e.g. by using a **hardware security module..."** **10.2.5:** "... ensure these keys are **not exposed during transmission.** .... distributed to the intended recipient via an out-of-band channel or other secure means to **minimise the risk of interception..."**	• Provide an additional layer of protection beyond the physical security controls with **Secure Transport Mode** – the logical control validation capability. Utilize 'Secure Transport Mode' to **logically lock the HSM during shipment.** Upon receipt, administrators can cryptographically verify that the device has not been tampered with or modified before deploying it into production. • Establish **secure, authenticated communication channels** for key management and cryptographic operations, using protocols compliant with standards such as NIST SP 800-56A/B and RFCs for TLS, SSH, and IPsec. • 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.	
11. Data and Infrastructure Security		
11.1 – Data Security **11.1.1:** "... develop comprehensive data loss prevention policies and adopt measures **to detect and prevent unauthorised** access, modification, copying, or transmission of its confidential data, taking into consideration the following: **(a) data in motion;** **(b) data at rest; and** **(c) data in use.** **11.1.2:** "... implement appropriate measures to **prevent and detect data theft,** as well as **unauthorised modification** in systems and endpoint devices... **ensure** systems managed by the **FI's service providers** are accorded the same level of protection and subject to the **same security standards.** **11.1.6:** The use of **sensitive production data in non-production** environments should be restricted... ensure **appropriate controls** are implemented in non-production environments to manage the access and removal of such data to prevent data leakage. Where possible, such **data should be masked in the non-production environments.**	• Identify the current state of **data compliance and document gaps.** • **Encrypt data at rest** on-premises, across clouds, and in big data or container environments. • 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. • Provide **on-premises solutions** for data discovery, classification and protection to FIs to achieve "same security standards". • **Pseudonymize sensitive data** once it is created and make sure cleartext data will not be processed or stored by unauthorized and to prevent exposure of real data applications and personnel. • **Protect the root-of-trust** of a cryptographic system within FIPS140-3 Level 3 - a highly secure environment. • **Protect data in motion** with high-speed encryption. • **Protect data in use** by leveraging confidential computing.	**Data Security** • Data Activity Monitoring • Data Discovery & Classification • Data Risk Analytics • File Activity Monitoring • High-Speed Encryption • Hardware Security Modules • Tokenization • Transparent Encryption

Guidelines	How Thales Helps	Solution Areas
	• **Examine application and database traffic** automatically to create a profile of baseline normal activity. • Gain **full sensitive data activity visibility**, track who has access, audit what they are doing and document. • Pinpoint **risky data access activity** for all users, including privileged users. • Protect data with **real-time alerting or user access blocking** of policy violations.	
11.1.3: "... confidential data stored in **systems and endpoint devices** should be encrypted and protected by **strong access controls..."**	• 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 authorization 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.	**Data Security** • Data Activity Monitoring • Data Risk Analytics • Transparent Encryption **Identity and Access Management** • Identity Verification • Multi-Factor Authentication • Thales OneWelcome Identity Platform • Workforce Access Management
11.2 Network Security **11.2.1:** "... install **network security devices** such as firewalls to secure the network ... the Internet, as well as connections with third parties..." **11.2.2:** "... deploy effective security mechanisms **to protect information assets**...grouped into network segments based on the criticality of systems, the system's functional role (e.g. database and application) or the sensitivity of the data..."	• 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. • **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. • Provide instant protection against both **volumetric and application-layer** DDoS attacks in one solution.	**Application Security** • DDoS Protection • Cloud Web Application Firewall **Data Security** • Discovery and Classification

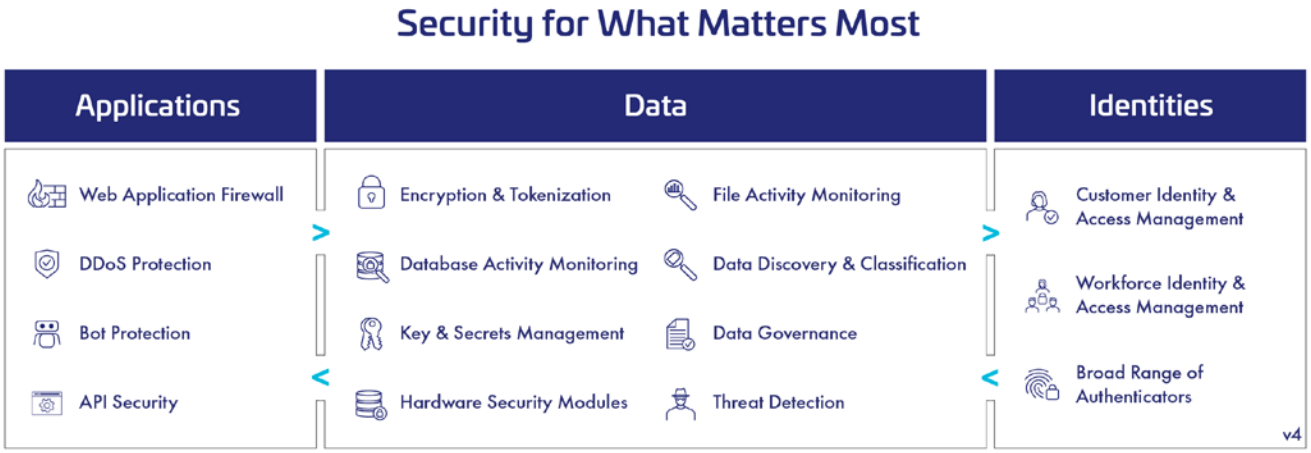
Guidelines	How Thales Helps	Solution Areas
11.2.3: "...Network intrusion prevention systems should be deployed ... to **detect and block malicious network traffic..."** **11.2.7:** "...An **effective DoS protection** should be implemented to detect and respond to various types of DoS attacks.... engage DoS mitigation service providers to filter potential DoS traffic..."	• Leverage 60+ global PoPs to absorb large attacks, avoiding costly hardware or over-provisioning—**elastic defense scales** automatically.	
11.3 – System Security **11.3.7:** "When implementing **Bring Your Own Device (BYOD)** ... should conduct a comprehensive risk assessment and implement appropriate measures to **secure its BYOD environment** ... use their personal devices to access the corporate network." **Annex B: BYOD Security**	• Control and manage access to IT systems from external networks (teleworking) by supporting **Multi-Factor Authentication** (MFA) and **Risk-Based Authentication.** • Set policies for **administrators to approve connections from external networks** and display results as remote access activity reports. • Manage **access policies for mobile devices,** such as checking security patch installations and device settings, and enforcing antivirus and malware policies. • **Check devices before granting access** to IT systems in cases where employees are allowed to use BYOD, such as preventing connections from rooted or jailbroken devices and forcing the installation of updated anti-malware to prevent threats from personal devices.	**Identity and Access Management** • Adaptive Access Control • Fraud & Risk Management • Multi-Factor Authentication • Risk-Based Authenticationw
11.4 – Virtualisation Security **11.4.2: "Strong access controls** should be implemented to **restrict administrative access** to the hypervisor and host operating system ... in the virtual environment."	• Integrate **key management with VMware** to enable VM image encryption and VSAN encryption. • Enable data inside VMs and containers to be secured via **encryption and access control** transparently without any changes to the application.	**Data Security** • Key Management • Hardware Security Modules • Transparent Encryption
12. Cyber Security Operations		
12.2 – Cyber Event Monitoring and Detection **12.2.2:** "A process to collect, process, review and retain **system logs**... to facilitate the FI's security monitoring operations. These logs should be protected against unauthorised access."	• **Produce audit trail and reports** of all access events to all systems, **stream logs** to external SIEM systems. • 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.	**Data Security** • Data Activity Monitoring • Data Risk Analytics **Identity and Access Management** • Adaptive Access Control • Multi-Factor Authentication • Risk-Based Authentication

Guidelines	How Thales Helps	Solution Areas
12.2.3: "... establish a **baseline profile** of each IT system's routine activities and analyse the system activities against the baseline profiles. The profiles should be regularly reviewed and updated." **12.2.4:** "... consider applying user **behavioural analytics** to enhance the effectiveness of security monitoring... might include the use of machine learning algorithms in real time to analyse system logs, **establish a baseline** of normal user activities and **identify suspicious** or anomalous behaviours." **12.2.5: "Correlation of multiple events** registered on system logs... to identify suspicious or anomalous system activity patterns..."	• Support the **creation of audit trail reports** of all accesses for auditing and investigation in the event of any incidents. • Flag **access anomalies** for investigation by the security team, and integrate seamlessly with SIEM solutions for a more comprehensive approach to threat and anomaly detection. • Examine application and database traffic automatically using **machine learning and behavioral analytics** to create a profile of baseline normal activity, and **detect and prioritize** anomalous activity. • **Offer correlation** with risk analytics that filters out false positives and enables security teams to act only on higher-risk incidents that need further investigation.	
13. Cyber Security Assessment		
13.1 – Vulnerability Assessment **13.1.1:** "... establish a process to conduct regular **vulnerability assessment** (VA) ... ensure risk arising from these gaps are addressed in a timely manner. The frequency of VA should be commensurate with the criticality of the IT system and the security risk to which it is exposed." **13.1.2:** "... the scope should minimally **include vulnerability discovery,** identification of **weak security configurations,** and open network ports, as well as **application** vulnerabilities. For web-based systems, the scope of VA should include checks on **common web-based 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. • Detect and virtually **patch database software vulnerabilities.**	**Data Security** • Data Activity Monitoring
14. Online Financial Services		
14.1 – Security of Online Financial Services **14.1.2:** "... secure its communications channels to protect customer data... can be achieved through **data encryption and digital signatures..."** **14.1.3:** "minimise exposure of the FI's online financial services to **common attack vectors** such as code injection attack, cross-site scripting, man-in-the-middle attack (MITMA),35 domain name system (DNS) hijacking,36 distributed denial of service (DDoS), malware and spoofing attacks..."	• **Encrypt all sensitive data** at both client and host applications prior to transmission using AES-256 or equivalent encryption standards. • Protect encryption keys associated with the **digital signatures** and secure cryptographic operations in a FIPS 140-3 Level 3 validated tamper-resistant device. • **Manage encryption keys** centrally, provide granular access control, and configure security policies.	**Application Security** • API Protection • Cloud Web Application Firewall • DDoS Protection **Data Security** • Data Activity Monitoring • Hardware Security Modules • Key Management • Transparent Encryption

Guidelines	How Thales Helps	Solution Areas
14.2 Customer Authentication and Transaction Signing **14.2.1: "Multi-factor authentication** should be deployed at login for online financial services ... can be based on two or more of the following factors, i.e. what you know (e.g. personal identification number or password), what you have (e.g. one-time password (OTP) generator) and who you are (e.g. biometrics)..." **14.2.2: "End-to-end encryption** should be implemented for the transmission of customer passwords ... To safeguard the confidentiality of customer passwords, the passwords should only be verified in a hardened or tamper resistant system..." **14.2.4:** "... implement appropriate risk-based or **adaptive authentication** ... commensurate with the risk level of the transaction and sensitivity of the data."	• Deploy a Mobile Strong Customer Authentication (SCA) solution that is designed to operate within a **secure and tamper-resistant runtime environment**, equipped with Run-time Application Self-Protection (RASP), device integrity checks, and anti-tampering controls to defend against malware, rooting/ jailbreaking, and unauthorized access. • Ensure **continuous mitigation** against emerging mobile application threats by providing mobile security that is periodically penetration-tested by independent third-party security labs. • Offer a Mobile SCA solution that is strictly **prohibited from storing sensitive** authentication data such as PINs and passwords on the device. • Enable activation of the mobile authenticator only after **strong identity verification** by the bank. Cryptographic keys are securely transmitted via end-to-end encrypted channels to prevent interception or manipulation. • Support **strong device binding** between the customer's device and the user's cryptographic key is enforced during the provisioning stage, effectively preventing unauthorized installations or cloning attempts.	**Identity and Access Management** • Strong Customer Authentication
14.3 – Fraud Monitoring **14.3.1:** "... implement **real-time fraud monitoring** systems to identify and block suspicious or fraudulent online transactions..."	• Leverage advanced algorithms and machine learning to **analyze user** behavior, device fingerprints, location, and transaction patterns during online sessions, **identifying anomalies** before fraud occurs and automatically blocking high-risk access or transactions. • Provide **dynamic risk scoring** with >99% accuracy to distinguish legitimate users from threats and enabling automated actions. • Support multi-channel (mobile, web, desktop) **continuous monitoring compliant** with standards like PSD2 SCA and FFIEC, with customizable rules for FIs to enforce policies tailored to their transaction types and risk thresholds. • Use **anonymized global intelligence** from billions of events to flag devices/IPs linked to prior fraud, reducing manual reviews and ensuring proactive blocking of fraudulent online financial transactions.	**Identity and Access Management** • Fraud & Risk Management • Risk-Based Authentication

Guidelines	How Thales Helps	Solution Areas
15. IT Audit		
15.1 – Audit Function **15.1.1:** "...ensure **IT audit is performed** to provide the board of directors and senior management an independent and objective opinion of the adequacy and effectiveness of the FI's risk management, governance and internal controls relative to its existing **and emerging technology risks..."**	• Provide **audit trails** of API calls, authentication attempts, and authorization decisions, ensuring accountability and facilitating compliance audits. • Produce audit trail and reports of all **access events** to all systems, stream logs to external SIEM systems. • **Prevent unauthorized access** and alteration to its internals, including the audit logs. • Gain visibility by monitoring and **auditing all database activity.** • Provide a **clear audit trail** for demonstrating cryptographic control from centralized key management systems, logging all key lifecycle events such as key creation, rotation, and access. • Offer **encryption logs**, data access attempts, and encryption/decryption events, providing auditable proof of data protection **without application modifications.**	**Identity and Access Management** • Workforce Access Management

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



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

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

THALES

CYBERSECURITY

Contact us

For contact information, please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com