Compliance Brief

THALES

CYBERSECURITY

Complying with the Technology and Cyber Risk Management Guidelines in Cambodia

cpl.thalesgroup.com

THALES

CYBERSECURITY

The Technology and Cyber Risk Management Guidelines (TCRMG) issued by the National Bank of Cambodia (NBC) are a set of regulatory standards that require banks and financial institutions (BFIs) in Cambodia to strengthen their technology risk and cybersecurity posture across governance, operations, and resilience. The latest version, released in 2025, replaces the 2019 version and explicitly introduces "technology risk" and "cyber risk" into a single, mandatory, assessable framework for BFIs.

Purpose

- Help BFIs identify, assess, monitor, and mitigate operational, regulatory, and cyber risks arising from digital channels, IT infrastructure, third party vendors, and cloud services.

Scope

- Apply to all licensed Banking and Financial Institutions (BFIs) in Cambodia and expects controls to be proportionate to the complexity and risk profile of each institution.

How Thales Help with The Technology and Cyber Risk Management Guidelines in Cambodia?

Thales' solutions can help organizations address the requirements in five of the chapters by simplifying compliance and automating security with visibility and control, reducing the burden on security and compliance teams.

Guidelines	How Thales helps	Thales Solutions
Chapter 3 – IT Operation Management		
3.2 – Management of Information Assets **3.2.3:** "... new information assets and all existing **assets shall be inventoried... periodically update** ... categorize information assets into a minimum of three classification types: ..." **3.2.5:** "**Information assets classification** ... assign classes or levels of sensitivity and criticality to information assets .... define the level of access ..."	• **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**. • Discover and classify potential risk for all public, private and shadow **APIs**. • Provide **data activity monitoring** for structured and unstructured data across cloud and on-prem systems.	**Application Security** API Security **Data Security** Data Discovery & Classification Data Activity Monitoring Data Risk Analytics File Activity Monitoring
3.8 – Incident Management **3.8.8:** "... incorporating **DoS attack prevention** in their internet service provider (ISP) selection process..."	• Safeguard critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic.	**Application Security** DDoS Protection

Guidelines	How Thales helps	Thales Solutions
3.15 – Internet of Things **3.15.1:** "... maintain all IoT devices in information asset inventory ... such as their network **connections and physical locations**. **3.15.2:** "... assess and implement processes and strong **access controls ...**" **3.15.3:** "... ensure that IoT devices are installed on a **separate network segment** from ... critical and sensitive data..." **3.15.4:** "... IoT devices connecting to critical systems and confidential data are supported with **secure algorithm for protecting data at rest, in transit,** and in use from unauthorized access..."	• Manage authentication and access control by supporting **Multi-Factor Authentication** and displaying access log reports. • Set up access control policies based on user roles, responsibilities, and risks with **Adaptive Access Control**. • Protect personal data from **unauthorized access**, monitor what has been changed and who is accessing. • **Centralize authentication** and policy enforcement for cloud access scenarios, helping organizations apply consistent access controls. • Provide **ongoing monitoring** of database traffic, monitoring who the users are accessing them, and provide timely alerts. • Protect the root-of-trust of a **cryptographic system** within a highly secure environment. • **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 sensitive data with **real-time alerting or user access blocking** of policy violations. • Protect **data in motion** with high-speed encryption.	**Data Security** Data Activity Monitoring Data Risk Analytics Hardware Security Modules High-Speed Encryption Transparent Encryption Tokenization **Identity & Access Management** Adaptive Access Control Multi-Factor Authentication
Chapter 4 – Cybersecurity Management		
4.3 – Access Control **4.3.1:** "... establish and review **an access control policy and procedures** based on business and information..." **4.3.2:** "... **procedure shall cover**, but not be limited to..." • "Access right provisioning ... review..." • Proxy or ad hoc user access provisioning and de-provisioning; • "Deactivation of user IDs associated ..." • "Modification of user access rights ... a change in roles..." • "Revocation of user access..." • "Prompt notification ... any additions, deletions, or changes in user roles or profiles..." • Access control matrix review. **4.3.3:** "... implement role-based access control (**RBAC**) and apply the principle of least privilege ..." **4.3.4:** "... establish an **access control matrix** that details roles or profiles and their associated permissions..." **4.3.10:** "... personnel with elevated or **high privilege access** shall be closely supervised ..."	• 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. • Offer 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. • 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. • Offer "**least privilege**" access rights where the minimum sufficient permissions are granted to legitimate users. • 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.	**Data Security** Data Activity Monitoring Data Risk Analytics Transparent Encryption **Identity & Access Management** Authentication Service – Private Cloud Identity Verification Multi-Factor Authentication Thales OneWelcome Identity Platform SafeNet Trusted Access (STA) Workforce Access Management

Guidelines	How Thales helps	Thales Solutions
4.5 – Cryptography **4.5.8:** "... use **key management system** based on..." • "Generating keys for different cryptographic systems ..." • "...obtaining public key certificates..." • "Distributing keys ..." • "... storing keys and ... access controls..." • "... rules for changing or updating keys..." • "Revoking and recovering of keys ..." • "Backing up or archiving keys ..." • "...destroying keys ..." • "Logging and auditing ..." **4.5.9:** "...assess the suitability of using **digital signatures** ..." **4.5.10:** "... digitally signed documents ... **transmitted over a secure channel** ..." **4.5.11:** "... ensure that the **digital signing process** ... is clearly explained and comprehensible to customers..."	• **Support cryptography algorithms** such as Advanced Encryption Standard (AES) 256bits, RSA 3072 bits, and are designed for a **post-quantum upgrade** to maintain crypto-agility. • **Manage encryption keys**, provide granular access control and configure security policies. • **Centralize key lifecycle management**, including generation, rotation, destruction, import, and export. • Ensure **secure deletion** by removing keys from CipherTrust Manager, digitally shredding all instances of the data. • **Protect cryptographic keys** in a FIPS 140-3 Level 3 environment. • Easily **back up and duplicate sensitive** cryptographic keys securely to the FIPS 140-3 Level 3 certified backup HSM. • Manage and protect **all secrets and sensitive credentials**. • **Protect data in motion** with high-speed encryption.	**Data Security** Hardware Security Modules High-Speed Encryption Key Management Transparent Encryption
4.9 – Data Security **4.9.1:** "... establish a **data security policy and procedures** to safeguard sensitive or critical data/ information ..." **4.9.2:** "... **data security procedures** shall cover, but not be limited to: • "Roles and responsibilities for data security ..." • "Data/information classification ... levels of sensitivity and criticality..." • "Secure data handling throughout data lifecycle..." • "Data security training and awareness..." **4.9.3:** "... ensure that **full disk encryption** is implemented on endpoint devices and removable media that store confidential data/ information..."	• **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**. • 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 financial institutions at risk. • Detect and report non-compliant, risky, or **malicious data access** behavior across all your data repositories enterprise-wide to accelerate remediation. • Categorize and prioritize by **real risks** with risk scoring rather than anomalies. • Adopt **transparent and continuous encryption** that protects sensitive data. • Securely manage encryption keys for **on-premises FDE storage**. • Ensure **secure deletion** by removing keys from CipherTrust Manager, digitally shredding all instances of the data.	**Data Security** Data Activity Monitoring Data Risk Analytics Discovery & Classification Hardware Security Modules Key Management Transparent Encryption

Guidelines	How Thales helps	Thales Solutions
4.9.5: "... ensure that **confidential data is encrypted** using industry-standard methods both in transit and at rest..." **4.9.6:** "... implement **data security techniques**, such as data masking, anonymization, pseudonymization, and tokenization, to safeguard confidential data..." **4.9.8:** "... restrict sensitive production data in **non-production environments**... such data needs to be used in non-production environments... **data security techniques** shall be applied..." **4.9.10:** "... consider implementing **appropriate technologies**... The state of data protection shall cover the following: • Data at rest • Data in transit • Data in use	• 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** 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 FIPS 140-3 Level 3 - a highly secure environment. • **Protect data in motion** with high-speed encryption. • **Protect data in use** by leveraging confidential computing. • **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.	**Data Security** Data Activity Monitoring Data Risk Analytics Discovery & Classification File Activity Monitoring High-Speed Encryption Hardware Security Modules Tokenization Transparent Encryption

Guidelines	How Thales helps	Thales Solutions
6.1 – Internet Banking **6.1.1:** "... implement at least **two-factor authentication** to validate customers' identities... to conduct any online transaction..." **6.1.2:** "... ensure that secure authentication such as **one-time password (OTP)** ... has a limited validity period for each financial transaction... using a secure, unpredictable algorithm and delivered via a secure channel..." **6.1.3:** "... implement web application firewall (**WAF**) to protect against Denial of Service (DoS) attacks..."	• Deploy MFA to ensure **proper customer authentication and authorization** when changing transaction limits or performing other sensitive account activities. • Deploy MFA, leveraging **FIDO authentication**, strong device binding, transaction signing, risk-based authentication, and cryptographic protections (e.g. Run-time Application Self-Protection) throughout the authentication execution. • Provide **FIDO authentication** that validates the authenticity of the website domain during the login process, ensuring that customers are interacting only with the genuine financial institution site and preventing credential phishing or redirection attacks. • Support **time-bound OTP generation** that aligns with OATH/OCRA standard. • Deploy **OTP** that is cryptographically bound to specific transaction details (transaction signing), ensuring that it can only be used for the intended transaction. • Perform all transactions and data exchanges over **TLS minimally**, with additional end-to-end **encryption layer** for sensitive information, such as user's key and/or password. • **Encrypt all sensitive data** at both client and host applications prior to transmission using AES-256 or equivalent encryption standards. • Implement mutual TLS to **authenticate the connection** between endpoints and the server that hosts the solution. • Deliver high security efficacy by **blocking threats** such as SQL injection, XSS, and other OWASP Top 10 vulnerabilities with WAF. • Safeguard critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic. • Provide instant protection against both **volumetric and application-layer** DDoS attacks in one solution. • Leverage 63 global PoPs to absorb large attacks, avoiding costly hardware or over-provisioning—**elastic defense scales** automatically.	**Application Security** API Security Bot Protection DDoS Protection Web Application Firewall **Identity & Access Management** Fido Devices Solution Fraud and Risk Management Identity Verification Multi-Factor Authentication Strong Customer Authentication

Guidelines	How Thales helps	Thales Solutions
6.2 – Mobile Banking **6.2.1:** "... implement at least **two-factor authentication** ... requires customers to provide both a password and additional authentication ..." **6.2.2:** "... implement a secure and reliable time-based one-time password (**TOTP**) mechanism ... delivered to user via a secure channel..." **6.2.3:** "... implement **multi-factor authentication** for high-value fund transfers ..." **6.2.4:** "... ensure the integrity and authenticity of the **mobile application...**" **6.2.5:** "... implement code **minification** and code **obfuscation** techniques to prevent reverse engineering ..." **6.2.6:** "... implement security measures to **detect and prevent installation** of the mobile application on emulators and jailbroken or rooted devices. **6.2.7:** "... implement web application firewall (**WAF**) to protect against **DoS attacks**, including rate limiting ... traffic filtering, and anomaly detection to identify and mitigate unusual patterns ..." **6.2.8:** "... made available only through **trusted** mobile application **repositories**..."	• Provide **robust customer authentication and identity verification** processes, including multi-factor authentication (MFA) for activation of digital services, passive liveness that is compliant to iBETA PAD Level 2. • Support **time-bound OTP generation** that aligns with OATH/OCRA standard. • Deploy **strong device binding** to ensure the user's credentials or cryptographic keys are securely linked to the device. • Identify **behavioral or anomaly detection** mechanisms, events such as new device access or unusual location changes, triggering immediate customer notification or further verification actions from the Bank's resource. • Enable **MFA validation** for registering a new or replacement mobile number, device change, or processing personal particulars updates. Additional identity verification or part of KYC procedures may be applied when necessary to ensure authenticity. • Apply **systematic risk management** controls to detect multiple successive high-volume transactions or abnormal transaction patterns, enabling proactive fraud mitigation. • Include secure session handling, automatic timeouts, and **protection against session hijacking** or replay attacks. • Detect and limit repeated failed login or MFA authentication attempts to **prevent brute-force** and credential-stuffing attacks. • Safeguard critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic. • Inspect all traffic, detect and **prevent web-based attacks** with WAF. • Provide a **highly secure environment** that is resistant to phishing, malware, and man-in-the-middle attacks with a combination of Strong Customer Authentication (SCA), Risk Management solution, FIDO authentication, device binding, and Run-time Application Self-Protection (RASP). • Ensure accuracy and reliability in customer authentication through the **advanced biometric verification** with a low False Acceptance Rate (FAR).	**Application Security** API Protection Bot Protection DDoS Protection Web Application Firewall **Identity & Access Management** FIDO Devices Solution Fraud and Risk Management Identity Verification Multi-Factor Authentication Strong Customer Authentication

Guidelines	How Thales helps	Thales Solutions
6.5 – Payment Cards **6.5.1:** "... use the Payment Card Industry Data Security Standard (**PCI DSS**) ... for compliance assessment..." **6.5.2:** "... ensure **full compliance** with payment card security requirements..." **6.5.3:** "... implement the **EMV standard** for payment cards..." **6.5.4:** "...implement **secure authentication** methods for card-not-present transactions ... via the Internet..." **6.5.5:** "... promptly notify cardholders through **transaction alerts** whenever transaction is made on their payment cards..." **6.5.6:** "... implement robust **fraud detection** systems to identify, detect and prevent fraudulent activities..." **6.5.7:** "... set out **risk management** parameters according to risks posed by cardholders ... to enhance fraud detection capabilities..." **6.5.8:** "... **monitor** and investigate **transactions** that significantly deviate from a cardholder's usual usage..."	• FIPS 140-2 Level 3 **root of trust** for credentials and keys. • **Support cryptography algorithms** such as Advanced Encryption Standard (AES) 256bits, RSA 3072 bits, and are designed for a **post-quantum upgrade** to maintain crypto-agility. • Detect and limit repeated failed login or MFA authentication attempts to **prevent brute-force** and credential-stuffing attacks. • Deploy MFA to ensure **proper customer authentication and authorization** when changing transaction limits or performing other sensitive account activities. • Identify **behavioral or anomaly detection** mechanisms, events such as new device access or unusual location changes, triggering immediate customer notification or further verification actions from the Bank's resource. • Apply **systematic risk management** controls to detect multiple successive high-volume transactions or abnormal transaction patterns, enabling proactive fraud mitigation. • Adjust **access permissions** based on real-time or near real-time user behavior and contextual factors. • Apply **Strong Customer Authentication** (SCA) to all financial and high-risk non-financial transactions. It leverages FIDO authentication, biometrics, or OTP-based validation to ensure the authenticity of the user, device, and transaction integrity. • Adopt SCA that requires users to **review and confirm transaction** details (e.g. payee information, amount, and destination account). • Offer **multiple MFA options** that are more secure than SMS OTP, such as OTP/OATH authenticator, FIDO authenticator, and Risk-Based Authentication. • Fully **support transaction signing**, whereby the authentication code is uniquely tied to the confirmed beneficiary and transaction amount. • Deploy **Mobile Secure Messenger** – a secure channel for sending push notifications.	**Data Security** Hardware Security Modules **Identity & Access Management** Adaptive Access Control FIDO Devices Solution Fraud and Risk Management Identity Verification Mobile Secure Messenger Multi-Factor Authentication Strong Customer Authentication
6.6 – SWIFT **6.6.1:**" ... use the latest SWIFT Customer Security Controls Framework (**CSCF**) to perform their compliance assessment..." **6.6.2:** "... ensure full compliance with all mandatory requirements of the **SWIFT CSCF**..."	• Provide a hardened, **tamper-resistant** environment for secure **cryptographic processing**, key generation and protection, encryption, and more to address the CSCF requirements. • Protect **cryptographic keys** in a FIPS 140-2 Level 3 environment.	**Data Security** Hardware Security Modules

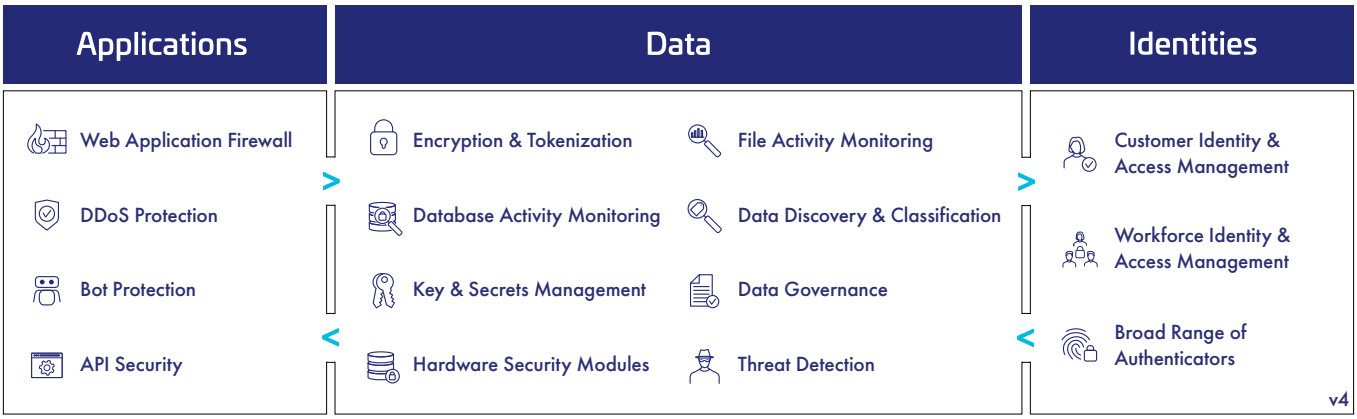
Guidelines	How Thales helps	Thales Solutions
Chapter 7 – Technology Service Outsourcing		
7.0.11: "... ensure that the **storage of its data** is at least logically segregated from the other clients of the third-party service provider... In the event of termination of outsourcing agreement ... ensure that all confidential data is retrieved and destroyed from the service provider..."	• **Retain full control and ownership** of the sensitive data by controlling encryption keys access via Cloud Key Management, negating the risk of data being released to third party with the **Hold-Your-Own-Key (HYOK)** approach. • Secure sensitive data for migration by **encrypting data-at-rest** on-premises, across clouds, and in big data or container environments. • Allow **encrypted data to be migrated between different clouds**, removing any reliance on specific formats used by different cloud providers; customers are not locked to a single cloud. • Ensure **secure deletion** by removing keys from CipherTrust Manager, digitally shredding all instances of the data. • **Pseudonymize** sensitive information in databases. • 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 authorization.	**Data Security** Cloud Key Management Key Management Transparent Encryption Tokenization **Identity & Access Management** Delegated User Management Externalized Authorization Third-party Access Control
Chapter 8 – Enabling Technologies		
8.1 – Cloud Computing **8.1.9:** "...maintain an asset inventory of all systems hosted on cloud services with clear ownership..." **8.1.10:** "...implement multi-factor authentication for users with privileges to configure cloud services..." **8.1.13:** "... hardware security module (HSM) is used for generating, storing, and managing the keys and is hosted in a higher control environment (e.g., own on-premise IT infrastructure) rather than with the CSP..."	• **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 in the cloud. • Provide **data activity monitoring** for structured and unstructured data across cloud. • Secure sensitive data and **maintain complete governance and control** of sensitive data and the associated encryption keys and policies with Bring-Your-Own-Encryption (BYOE), Hold-Your-Own-Key (HYOK) and Bring-Your-Own-Key (BYOK) approaches, as well as a centralized multi-cloud key management. • 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**. • Accelerate threat detection and ease forensics with **data access audit logging**. • Employ **strong, standards-based encryption protocols**, such as the Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key exchange. • **Simplify key management** across on-premises and multi-cloud deployments by centralizing control on the FIPS 140-2 Level 3 environment. • Employ a **Role-Based Access Control (RBAC)** to control access to Hardware Security Modules (HSMs) and broader key management systems to ensure that only authorized personnel can perform specific administrative or cryptographic tasks, maintaining a strict **separation of duties**. • 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 authorization.	**Data Security** Cloud Key Management Data Activity Monitoring Discovery & Classification Hardware Security Modules High-Speed Encryption Tokenization Transparent Encryption **Identity & Access Management** Delegated User Management Externalized Authorization SafeNet Trusted Access Third-party Access Control

Guidelines	How Thales helps	Thales Solutions
8.2 – Application Programming Interface **8.2.4:** "... implement detective measures, including real-time monitoring and alerting technologies, to track API usage, monitor performance, and detect suspicious activities..."	• **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** API Security Attack Analytics Bot Protection DDoS Protection Web Application Firewall
8.5 – Distributed Ledger Technology and Blockchain Technology **8.5.1:** "...establish, and review **secure key management** procedures..." **8.5.2:** "...implement **robust security** measures ... against unauthorized access and cyber threats..." **8.5.3:** "... implement a secure **identity and access management** ..." **8.5.4:** "... implement **fraud prevention** measures ..." **8.5.5:** "...smart contracts ... conduct and evaluate a security assessment and auditability ... does not contain **vulnerabilities**..." **8.5.6:** "...periodically perform **security assessment** ... to identify and remediate potential vulnerabilities..." **8.5.7:** "... implement private/ permissioned DLT/BT systems that... only **authorized entities** within the designated network..." **8.5.8:** "...implement **secure consensus algorithm** for DLT/BT platform ..."	• Offer FIPS 140-2 Level 3 **root of trust** for credentials and keys. • Provide future-proof and standardize **quantum-safe digital signature algorithms**. • Generate digital signatures seamlessly using standardized **quantum-safe public key cryptography** and includes key management capabilities for stateless and stateful key types, complying with SP 800-208 requirements. • Manage **seeds and private keys** securely with HSMs. • Access to these HSMs is tightly controlled, with **strong multi-factor authentication** and detailed audit trails for all operations. • Secure **sensitive data and critical applications** by storing, protecting, and managing cryptographic keys – high assurance, tamper-resistant, network-attached appliances offering market-leading performance. • **Backup easily and duplicate keys** securely for compliance as well as safekeeping in case of emergency, failure or disaster.	**Data Security** Hardware Security Modules

Guidelines	How Thales helps	Thales Solutions
8.6 – Tokenization **8.6.1:** "... establish and review secure **token management** procedures..." **8.6.2:** "... ensure the tokenization system ... to be **resilient and secure** against reverse-engineering ..." **8.6.3:** "... tokenization system is implemented in accordance with **industry standards** ..." **8.6.5:** "...ensure that the token vault ... is protected with **secure encryption and access controls**..." **8.6.6:** "... ensure that the tokenization system ... **maintains logging** of all activities..." **8.6.8:** "... ensure that the **token service provider** ... has access to only the token and **not the original data**..."	• **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. • Utilize Hardware Security Modules (HSMs) with FIPS 140-2 Level 3 validation as **the root of trust**. • **Secure access** to decrypted data across environments due to centralized management. • **Maintain control** in the cloud and cloud providers never have access to token vaults or keys.	**Data Security** Hardware Security Modules Tokenization

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.