

Complying with the Guidelines for the Provision of Information Technology Systems by SEC of Thailand

The Guidelines for the Provision of Information Technology Systems ([แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ นป. 6/2567](#)) issued by the Securities and Exchange Commission of Thailand (SEC) are designed to ensure that financial institutions, securities companies, and other regulated entities maintain secure, reliable, and efficient IT systems. The guidelines are part of Thailand's broader regulatory framework aimed at strengthening cybersecurity, data protection, and operational resilience in the capital markets.

What are the Guidelines for the Provision of Information Technology Systems in Thailand?

1. Regulatory Authority:

- The Securities and Exchange Commission of Thailand (SEC) oversees securities and capital market operations, including IT governance for financial service providers.
- These guidelines align with Thailand's Cybersecurity Act B.E. 2562 (2019) and Personal Data Protection Act (PDPA).

2. Purpose:

- To mitigate risks related to IT system failures, cyber threats, and data breaches.
- To ensure confidentiality, integrity, and availability (CIA triad) of financial data.

- To promote business continuity and disaster recovery preparedness.

3. Scope:

- Applies to securities firms, asset managers, crowdfunding platforms, and other SEC-regulated entities.
- Covers IT infrastructure, so

How Thales Helps with The Guidelines for the Provision of Information Technology Systems in Thailand

Thales' solutions can help organizations address 6 requirements in Chapter 2 – Information Technology Security by simplifying compliance and automating security with visibility and control, reducing the burden on security and compliance teams.

Guidelines	How Thales helps	Thales Solutions
2.2 Human Resource Management and External Personnel		
2.2.2 "Third-party management External persons who must be managed 2.2 External Persons in the event of any of the following actions: <ul style="list-style-type: none"> • 2.2.1 Using IT services • 2.2.2 Connecting the IT system • 2.2.3 Allowing external persons to access important information or customer information in electronic form..." 	<ul style="list-style-type: none"> • Manage system and data access rights (access control) by supporting role-based authorization (RBAC) and conditional authorization (ABAC). • Offer Delegated User Management to grant or revoke rights quickly with audit trail. • Manage user authentication process by supporting multi-factor authentication (MFA). • Control and manage privileged user accounts by supporting the enforcement of multi-factor authentication (MFA) for accessing critical systems. • Manage and control external access (third-party access management) by supporting authentication via social media or original organization accounts (BYOI). • Assess risks before logging in and check access risks in real time (Risk-Based Authentication), including displaying as a third-party access audit report to enable continuous monitoring, auditing, and supervision. 	Identity & Access Management Adaptive Access Control BYOI & Social Login Delegated User Management Externalized Authorization Multi-Factor Authentication Risk-Based Authentication

Guidelines	How Thales helps	Thales Solutions
2.4 Data Security		
4.2 Data Classification and Data Security Guidelines		
1. "... define data classification criteria and data handling methods according to the level of confidentiality... "	<ul style="list-style-type: none"> • Identify structured and unstructured sensitive data at risk across Hybrid IT. • 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. • Discover and classify potential risk for all public, private and shadow APIs. 	Application Security API Security Data Security Data Discovery & Classification
2. "Define data security measures in line with the level of confidentiality , covering: 1) Data on devices used for operations (data at the endpoint) 2) Data in transit (data in transit) 3) Data on the work system and data storage media (data at rest)..."	<ul style="list-style-type: none"> • Detect and prevent cyber threats with web application firewall, ensuring seamless operations and peace of mind. • Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic. • Provide uptime with fast, effective DDoS mitigation and a 3-second SLA for Layers 3 & 4 attacks. • Protect against business logic attacks and many more of the OWASP API Top Ten threats. • Provide continuous protection of all APIs using deep discovery and classification to detect all public, private and shadow APIs. 	Application Security API Security Attack Analytic Bot Protection Web Application Firewall
	<ul style="list-style-type: none"> • 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. 	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	Thales Solutions
2.5 Access Control of Information and IT Systems		
<p>5.1 "...Provide guidelines for managing user accounts and access rights... including a process for revoking rights when no longer needed..."</p> <p>5.2 "Provide an authentication process appropriate to the risk and prevent denial of liability."</p> <p>5.3 Establish measures to control, limit, and monitor the use of privileged user accounts...</p> <p>5.3.1 "...Have MFA when logging in and changing passwords for ... significant IT systems..."</p> <p>5.3.2 "In cases where business operators have limitations on MFA ... and risk assessments and risk control measures must be conducted before requesting exceptions..."</p> <p>5.3.3 Strict control and monitoring of privileged user account usage.</p>	<ul style="list-style-type: none"> • Manage system and data access rights (access control) by supporting role-based access control (Role-Based Access Control: RBAC). • Offer decentralized user rights (Delegated User Management) by quickly granting or revoking rights and produce audit log for access change. • Provide user authentication processes by supporting multi-factor authentication, risk assessment before logging in (Risk-Based Authentication) and single signon (Single Sign-On: SSO) with audit trail report of login activity reports. • Control and manage privileged user accounts with multi-factor authentication, accessing critical systems. • Use MFA-equivalent authentication processes, such as device binding or biometric authentication. • Perform risk assessment before approving exceptions, and store evidence of exceptions in the form of exception approval reports to comply with policies. 	<p>Identity & Access Management</p> <p>Delegated User Management</p> <p>Multi-Factor Authentication</p> <p>Risk-Based Authentication</p>
2.6 Cryptographic Control		
<p>6.1 Define secure encryption methods</p> <p>1. "... business operators should do at least the following:</p> <p>"2) Define data encryption method standards (cryptographic algorithm) to be in accordance with international standards ..."</p>	<ul style="list-style-type: none"> • Protect cryptographic keys in FIPS-validated and tamper-evident hardware. • Encrypt keys with a one-time-use AES 256 key and sent over a mutually authenticated TLS connection. • Adopt transparent and continuous encryption that protects against unauthorized access by users and processes in physical, virtual, and cloud environments. • Employ strong and standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange. 	<p>Data Security</p> <p>Hardware Security Modules</p> <p>Key Management</p> <p>Transparent Encryption</p>

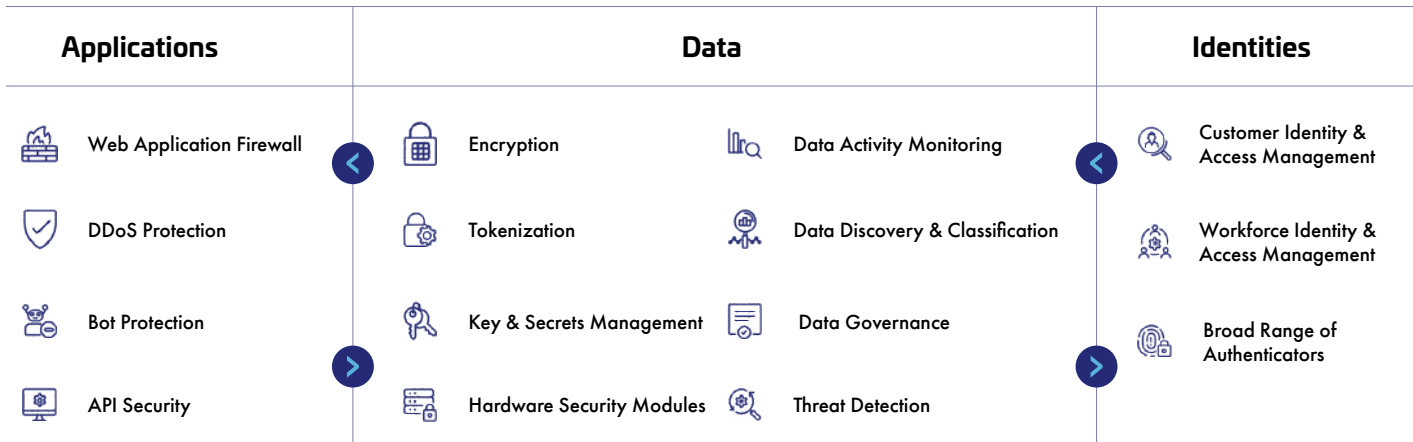
Guidelines	How Thales helps	Thales Solutions
<p>6.2 Define the management of encryption keys by providing control measures from:</p> <p>1. Creating and installing encryption keys:</p> <p>2) "Set access rights to the encryption keys ..."</p> <p>3) "Set the length of the encryption keys ..."</p> <p>4) "Exchange encryption keys through secure processes and channels."</p> <p>2. Storage and backup of encryption keys:</p> <p>1) "Secure the storage of encryption keys ... such as using Hardware Security Module (HSM) devices ..."</p> <p>2) "Backup the encryption keys ... with the same level of security as the main encryption keys..."</p> <p>3. Revocation or destruction of encryption keys:</p> <p>1) "Set criteria and guidelines for changing and revoking encryption keys..."</p> <p>2) "Establish a process for destroying keys ..."</p> <p>4. "...keep logs of important events related to encryption keys ..."</p>	<ul style="list-style-type: none"> • Support cryptography algorithms such as Advanced Encryption Standard (AES) 256bits, RSA 3072 bits and 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 backup and duplicate sensitive cryptographic key securely to the FIPS 140-3 Level3 certified backup HSM. • Manage and protect all secrets and sensitive credentials. 	<p>Data Security</p> <p>Hardware Security Modules</p> <p>Key Management</p> <p>Secrets Management</p>
<p>6.3 Establish measures to control encryption keys provided by third parties</p> <p>1. "... take steps to ensure that the encryption keys provided by an external party are not shared with other service users and are secure, by considering the following ..."</p> <p>(1) Types of encryption keys</p> <p>(2) Details of the system and process for managing encryption keys</p> <p>(3) Recommendations for use and control of data encryption</p>	<ul style="list-style-type: none"> • 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. • Automate key lifecycle management across clouds and hybrid environments with processes and tools. • Enable relationship management with suppliers, partners or any third-party user; with clear delegation of access rights. • Minimize privileges by using relationship-based finegrained authorization. 	<p>Data Security</p> <p>Cloud Key Management</p> <p>Identity & Access Management</p> <p>Delegated User Management</p> <p>Third-party Access Control</p>

Guidelines	How Thales helps	Thales Solutions
<p>6.4 Establish a process to support the case of encryption key leakage.</p> <p>1. "... define the actions to be taken when an encryption key is leaked, such as contacting the agencies and people involved with the data set that uses the encryption key, checking the data set that is at risk of being leaked, changing or revoking the data encryption key, etc.</p>	<ul style="list-style-type: none"> • 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. 	<p>Data Security</p> <p>Key Management</p>
2.8 IT Operations Security		
2.8.5 Establishing policies and security measures for teleworking, mobile device use, and bring your own device (BYOD)		
<p>8.5 "...Establishing policies and security measures for teleworking, mobile device use, and bring your own device (BYOD)..."</p>	<ul style="list-style-type: none"> • Control and manage access to IT systems from external networks (teleworking) by supporting Multi-Factor Authentication (MFA) and Risk-Based Authentication. • 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 a 	<p>Identity & Access Management</p> <p>Adaptive Access Control</p> <p>Fraud & Risk Management</p> <p>Multi-Factor Authentication</p> <p>Risk-Based Authentication</p>
2.8.7 IT System Usage Event Log Storage		
8.7 IT system log storage (log) is complete and sufficient...		
<p>1. "... store log data in a secure manner ... and store for at least 90 days or as required by relevant laws..."</p>	<ul style="list-style-type: none"> • Record audit logs usage data and send usage data to SIEM system. 	<p>Data Security</p> <p>Data Activity Monitoring</p> <p>File Activity Monitoring</p>
<p>(1) Logs of entry and exit events of the computer center and areas related to the significant IT system (physical access log)</p>	<ul style="list-style-type: none"> • Manage authentication and access control by supporting Multi-Factor Authentication and Single Sign-On (SSO) and displaying access log reports. 	<p>Identity & Access Management</p> <p>Adaptive Access Control</p> <p>Multi-Factor Authentication</p> <p>Single Sign-On (SSO)</p>
<p>(2) "Authentication and access logs of the host computer, work systems, network devices and important data, including log-in attempts..."</p>	<ul style="list-style-type: none"> • Record access to the database system and detect login attempts on the database system. • Manage authentication and access control by supporting Multi-Factor Authentication. 	<p>Data Security</p> <p>Data Activity Monitoring</p> <p>File Activity Monitoring</p> <p>Identity & Access Management</p> <p>Multi-Factor Authentication</p>

Guidelines	How Thales helps	Thales Solutions
<p>(3) Significant activity logs, which at least cover:</p> <p>(a) "changes to the database structure (database schema log) and changes to data in important tables..."</p>	<ul style="list-style-type: none"> • Capture changes to the database structure (database schema log) and to data in important tables, which can be displayed as an access log table and as a report. • Produce audit trail and reports of all access events to all systems, stream logs to external SIEM systems 	<p>Data Security</p> <p>Data Activity Monitoring</p> <p>File Activity Monitoring</p>
<p>(4) "Evidence of electronic messaging conversations between access persons, ... and stored for at least 6 months..."</p>	<ul style="list-style-type: none"> • Provide control and audit access to electronic communication channels. 	<p>Identity & Access Management</p> <p>Adaptive Access Control</p>
<p>3. "... keep logs related to personal data for reviewing user activities and as evidence in case of inappropriate access, use, modification, or disclosure of personal data..."</p>	<ul style="list-style-type: none"> • Offer control and audit access to personal data (Personal Data Access Control) by supporting the setting of contextualized access policies (Adaptive Access Control) to suit the user's risk level. • Deploy Multi-Factor Authentication (MFA) for users accessing sensitive personal data or from new devices/locations. • Set prevention policies (Access Policies) for accessing sensitive data outside of business hours or from untrusted networks. • Detect and alert administrators if abnormal access attempts are found, and administrators can respond quickly. • Support the creation of audit trail reports of all accesses for auditing and investigation in the event of any incidents. 	<p>Identity & Access Management</p> <p>Adaptive Access Control</p>
<p>4. "... keep logs of important equipment on a separate logging server or use comparable methods that can prevent changes, modifications, or destruction of logs..."</p> <p>(1) "Define the duties and responsibilities of those who can access logs ..."</p> <p>(2) Have a strict process for verifying identity and checking access rights to logs.</p>	<ul style="list-style-type: none"> • Set access rights to the system log only for those who are authorized by roles and organization policies (Role-Based Access Control). • Control log access assignments in detail for auditing. • Enforce Multi-Factor Authentication (MFA) for administrators who need to access logs to increase security. • Offer strict audit log access rights using Adaptive Access Control to prevent unauthorized access and create Audit Trail records for retrospective auditing. 	<p>Identity & Access Management</p> <p>Adaptive Access Control</p> <p>Delegated User Management</p> <p>Multi-Factor Authentication</p>

Guidelines	How Thales helps	Thales Solutions
2.8.8 System Monitoring and Surveillance of Cyber Threats		
8.8 Security Monitoring		
4. [High Risk] "... have a system for collecting event data from various sources, ... in the process of linking data (log correlation) and analyzing unusual information security events."	<ul style="list-style-type: none"> • 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. • Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic. • Apply contextual security measures based on risk scoring. 	Application Security API Security Attack Analytic Bot Protection DDoS Protection Web Application Firewall
6. [High risk] "... have processes or tools to monitor and alert users of suspicious behavior ..."	<ul style="list-style-type: none"> • Alert or block database attacks and abnormal access requests in real time. • Monitor file activity over time to set up alerts on activity that can put financial institutions at risk. • Continuously monitor processes for abnormal I/O activity and alerts or blocks malicious activity. • 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. 	Data Security Data Activity Monitoring Data Risk Analytics Data Risk Intelligence File Activity Monitoring Transparent Encryption Ransomware Protection
2.8.9 Technical Vulnerability Assessment		
1. "... define the scope and frequency of technical vulnerability assessments to cover all systems according to the risk level..."	<ul style="list-style-type: none"> • Offer advanced API Verification capabilities to strengthen your defenses against potential vulnerabilities. 	Application Security API Security
2. "... assess the risk of the vulnerabilities found and determine a time frame for correction..." 3. "... report the results of the vulnerability assessments to the responsible person and follow up on the correction of vulnerabilities ..."	<ul style="list-style-type: none"> • 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. 	Data Security Data Activity Monitoring File Activity Monitoring
2.10 IT Project Management		
2.10.3 IT System Development		
(7) 1. "... important data from the real system is used to test the system ... should have guidelines to maintain the security and confidentiality of such data, such as data masking ..."	<ul style="list-style-type: none"> • Pseudonymize sensitive information in databases allows you to maintain control and compliance. 	Data Security Tokenization

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

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.

Disclaimer: The information contained herein is believed to be accurate on the date of publishing. Thales provides this material for your information only. Its content is not legal advice nor does it amount to a certification or guarantee of compliance in respect of any applicable law. Third parties shall be solely responsible for their own interpretation of any applicable law. The information should not be construed as a commitment to deliver any specific upgrade, feature or functionality. You should not rely on the anticipated timelines or potential upgrades, features or functionality described in the presentation when making a decision to purchase products from Thales. Thales does not accept any liability howsoever arising from any use of this material.