Compliance Brief

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

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ปม. 6/2567) ซึ่งออกโดยสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ของประเทศไทย มีเป้าหมายเพื่อให้สถาบันการเงิน บริษัทหลักทรัพย์ และหน่วยงานอื่นๆ ที่อยู่ภายใต้การกำกับดูแล สามารถรักษาระบบไอทีให้มีความปลอดภัย น่าเชื่อถือ และมีประสิทธิภาพ แนวปฏิบัติดังกล่าวเป็นส่วนหนึ่งของกรอบการกำกับดูแลที่กว้างขึ้นของประเทศไทย เพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ การคุ้มครองข้อมูล และความยืดหยุ่นในการดำเนินงานในตลาดทุน

แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของไทยคืออะไร?

1. วัตถุประสงค์

- เพื่อให้ผู้ประกอบธุรกิจต้องจัดให้มีการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและตรวจสอบด้านเทคโนโลยีสารสนเทศ ตลอดจนมีการทบทวนความเหมาะสมของเรื่องดังกล่าวเป็นประจำ

2. ขอบเขต

- บริษัทหรือสถาบันการเงินที่ได้รับใบอนุญาตให้ประกอบธุรกิจหลักทรัพย์ตามพระราชบัญญัติหลักทรัพย์ และตลาดหลักทรัพย์ พ.ศ. 2535

3. แนวทางปฏิบัติฯ

กำหนดแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศกับเรื่องดังต่อไปนี้

- การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)
- การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)
- การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)
- การทบทวนความเหมาะสมของการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ

Thales ช่วยเหลือตามแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของไทยได้อย่างไร?

โซลูชันของ Thales สามารถช่วยให้องค์กรต่าง ๆ ปฏิบัติตามข้อกำหนด 6 ประการในบทที่ 2 ของแนวปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศได้ โดยทำให้การปฏิบัติตามข้อกำหนดง่ายขึ้นและทำให้ความปลอดภัยเป็นไปโดยอัตโนมัติด้วยการมองเห็นและการควบคุมซึ่งช่วยลดภาระของทีมรักษาความปลอดภัยและการปฏิบัติตามกฎระเบียบ

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: • 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..."	• **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...**"	• **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**)..."	• 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
	• 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		
5.1 "...Provide guidelines for **managing user accounts and access rights...** including a process for revoking rights when no longer needed..." **5.2** "Provide an **authentication process** appropriate to the risk and prevent denial of liability." **5.3** Establish measures to control, limit, and monitor the use of **privileged user accounts**...: 5.3.1 "...Have **MFA** when logging in and changing passwords for ... significant IT systems..." 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..." 5.3.3 Strict control and monitoring of **privileged user account usage**.	• 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.	**Identity & Access Management** Delegated User Management Multi-Factor Authentication Risk-Based Authentication
2.6 Cryptographic Control		
6.1 Define **secure encryption methods** 1. "... business operators should do at least the following: "2) Define data encryption method standards (cryptographic algorithm) to be in accordance with international standards ..."	• **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.	**Data Security** Hardware Security Modules Key Management Transparent Encryption

Guidelines	How Thales helps	Thales Solutions
6.2 Define the management of encryption keys by providing control measures from: **1. Creating and installing encryption keys:** 2) "Set access rights to the encryption keys ..." 3) "Set the length of the encryption keys ..." 4) "Exchange encryption keys through secure processes and channels." **2. Storage and backup of encryption keys:** 1) "Secure the storage of encryption keys ... such as using **Hardware Security Module (HSM) devices** ..." 2) "Backup the encryption keys ... with the same level of security as the main encryption keys..." **3. Revocation or destruction of encryption keys:** 1) "Set criteria and guidelines for changing and revoking encryption keys..." 2) "Establish a process for **destroying keys** ..." 4. "...**keep logs** of important events related to encryption keys ..."	• **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.**	**Data Security** Hardware Security Modules Key Management Secrets Management
6.3 Establish measures to **control encryption keys** provided by **third parties** 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 ..." (1) Types of encryption keys (2) Details of the system and process for managing encryption keys (3) Recommendations for use and control of data encryption	• **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.	**Data Security** Cloud Key Management **Identity & Access Management** Delegated User Management Third-party Access Control

Guidelines	How Thales helps	Thales Solutions
6.4 Establish a process to support the case of **encryption key leakage.** 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.	• **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.	**Data Security** Key Management
2.8 IT Operations Security		
2.8.5 Establishing policies and security measures for teleworking, mobile device use, and bring your own device (BYOD)		
8.5 "...Establishing policies and security measures for teleworking, mobile device use, and bring your own device (**BYOD**)..."	• 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	**Identity & Access Management** Adaptive Access Control Fraud & Risk Management Multi-Factor Authentication Risk-Based Authentication
2.8.7 IT System Usage Event Log Storage		
8.7 IT system log storage (log) is complete and sufficient...		
1. "... **store log data** in a secure manner ... and store for at least 90 days or as required by relevant laws..."	• **Record audit logs** usage data and send usage data to SIEM system.	**Data Security** Data Activity Monitoring File Activity Monitoring
(1) **Logs of entry and exit** events of the computer center and areas related to the significant IT system (physical access log)	• Manage authentication and access control by supporting **Multi-Factor Authentication** and Single Sign-On (**SSO**) and displaying access log reports.	**Identity & Access Management** Adaptive Access Control Multi-Factor Authentication Single Sign-On (SSO)
(2) "**Authentication and access logs** of the host computer, work systems, network devices and important data, including log-in attempts..."	• **Record access** to the database system and detect login attempts on the database system. • **Manage authentication and access control** by supporting Multi-Factor Authentication.	**Data Security** Data Activity Monitoring File Activity Monitoring **Identity & Access Management** Multi-Factor Authentication

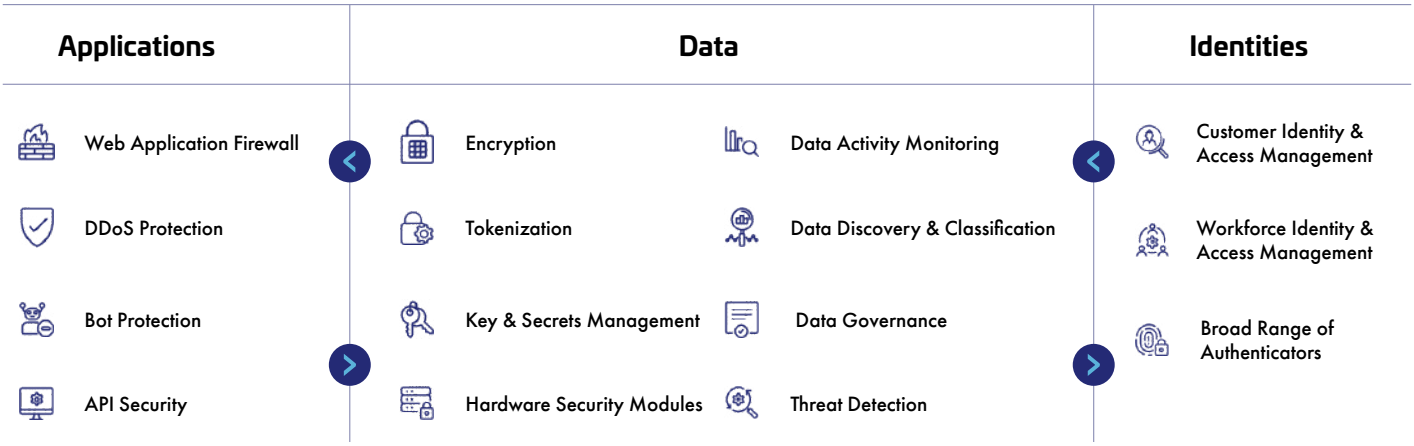
Guidelines	How Thales helps	Thales Solutions
(3) **Significant activity logs**, which at least cover: (a) "**changes to the database** structure (database schema log) and changes to data in important tables..."	• Capture **changes to the database** structure (database schema log) and to data in important 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	**Data Security** Data Activity Monitoring File Activity Monitoring
(4) "Evidence of electronic **messaging conversations** between access persons, ... and stored for at least 6 months..."	• Provide **control and audit access** to electronic communication channels.	**Identity & Access Management** Adaptive Access Control
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..."	• 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.	**Identity & Access Management** Adaptive Access Control
4. "... keep **logs of important equipment** on a separate logging server or use comparable methods that can **prevent changes, modifications, or destruction of logs**..." (1) "**Define the duties and responsibilities** of those who can access logs ..." (2) Have a strict process for **verifying identity** and checking access rights to logs.	• 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.	**Identity & Access Management** Adaptive Access Control Delegated User Management Multi-Factor Authentication
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."	• **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

Guidelines	How Thales helps	Thales Solutions
6. [High risk] "... have processes or tools to **monitor and alert users of suspicious** behavior ..."	• **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..."	• 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 ..."	• **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**..."	• **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.

THALES
Building a future we can all trust

imperva
a Thales company



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.