Compliance Brief

# Complying with the Information Technology Risk Management Guidelines by the Bank of Thailand (BOT)

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

**ธนาคารแห่งประเทศไทย (ธปท.) ได้มีการปรับปรุงหลักเกณฑ์ การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ฉบับปรับปรุงพุทธศักราช 2566 เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีการกำกับดูแลและบริหารจัดการเท่าทันความเสี่ยงจากการใช้เทคโนโลยีที่เปลี่ยนแปลงไป และเพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้เป็นแนวทางสำหรับการกำหนดวิธีปฏิบัติในการบริหารความเสี่ยงด้านเทคโน โลยีสารสนเทศ และการบริหารจัดการความเสี่ยงจากบุคคลภายนอก โดยเหมาะสมตามลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีที่นำมาใช้และความเสี่ยงที่เกี่ยวข้อง**

## แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ ธปท. คืออะไร?

### 1. วัตถุประสงค์

- กำหนดบทบาทหน้าที่ของหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์
- ส่งเสริมให้สถาบันการเงินและกลุ่มธุรกิจทางการเงินปฏิบัติตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้องได้อย่างถูกต้องและครบถ้วน

### 2. ขอบเขต

- สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง
- สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

### 3. แนวทางปฏิบัติฯ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีหน้าที่ต้องปฏิบัติตามหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

- ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)
- การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security management)
- การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)
- การปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)
- การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

## Thales ช่วยเหลือตามแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ ธปท. ได้อย่างไร

โซลูชันของ Thales สามารถช่วยองค์กรต่างๆ จัดการกับ 8 ข้อกำหนดในบทที่ 2 - ความปลอดภัยด้านเทคโนโลยีสารสนเทศโดยทำให้การปฏิบัติตามข้อกำหนดง่ายขึ้นและทำให้ความปลอดภัยเป็นไปโดยอัตโนมัติด้วยการมองเห็นและการควบคุม ซึ่งช่วยลดภาระของทีมรักษาความปลอดภัยและการปฏิบัติตามข้อกำหนดได้

| Description | How Thales helps | Thales Solutions |
|---|---|---|
| **2.2 Information Security** | | |
| 2.2.2 "Define the criteria for **information classification**, which should clearly state the **level of information confidentiality** (labeling)..." | • **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.<br>• Identify the current state of **compliance and document gaps**.<br>• Discover and classify potential risk for all public, private and shadow **APIs**. | **Application Security**<br>API Security<br><br>**Data Security**<br>Data Discovery & Classification |
| 2.2.3 "Establish guidelines for data security that are consistent with the level of confidentiality, covering:<br>- Data at **endpoint**<br>- Data in **transit**<br>- Data on systems and storage media (**data at rest**) ..." | • **Detect and prevent cyber threats** with web application firewall, ensuring seamless operations and peace of mind.<br>• Safeguard critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic.<br>• Deliver **unified protection**, with built-in detection and response for deprecated, unauthenticated, and **BOLA-prone APIs** and many more of the **OWASP API Top Ten threats**, stopping business logic abuse and API threats in real time.<br>• Provide **continuous protection of all APIs** using deep discovery and classification to detect all public, private and shadow APIs.<br>• **Encrypt data at rest** on-premises, across clouds, and in big data or container environments<br>• **Pseudonymize** sensitive information in databases.<br>• Protect the root-of-trust of a **cryptographic system** within a highly secure environment.<br>• Protect **data in motion** with high-speed encryption.<br>• Protect **data in use** by leveraging confidential computing.<br>• Gain full **sensitive data activity visibility**, track who has access, audit what they are doing and document. | **Application Security**<br>API Security<br>Attack Analytic<br>Bot Protection<br>DDoS Protection<br>Web Application Firewall<br><br>**Data Security**<br>Data Activity Monitoring<br>Data Discovery & Classification<br>Data Risk Analytics<br>File Activity Monitoring<br>High-Speed Encryption<br>Hardware Security Modules<br>Tokenization<br>Transparent Encryption |

| Description | How Thales helps | Thales Solutions |
|---|---|---|
| 2.2.5 "Establish standards and procedures for data destruction (**information disposal**) covering the scope of responsibility of relevant agencies, methods of data destruction consistent with the level of importance of the data..." | • Ensure **secure deletion** by removing keys from CipherTrust Manager, digitally shredding all instances of the data. | **Data Security**<br>Key Management<br>Transparent Encryption |
| 2.2.6 "Establish **standards and procedures for data encryption** management, covering the scope of responsibility of relevant agencies, **data encryption methods** (cryptographic algorithms) that are consistent with the level of data importance, and **data encryption key management** (key management)..." | • **Centralize key lifecycle management** tasks including generation, rotation, destruction, import and export.<br>• **Protect cryptographic keys** in a FIPS 140-2 Level 3 environment.<br>• Support cryptography algorithms such as Advanced Encryption Standard **(AES) 256bits, RSA 3072 bits** and designed for a **post-quantum upgrade** to maintain crypto-agility.<br>• Deploy **transparent encryption** for strong and **standard-based encryption protocols**.<br>• Manage and protect all **secrets and sensitive credentials**. | **Data Security**<br>Hardware Security Modules<br>Key Management<br>Transparent Encryption<br>Secrets Management |
| 2.2.7 "Data encryption methods should use reliable and **international data encryption standards**, such as symmetric data encryption (e.g. AES), asymmetric data encryption (e.g. public key cryptography), message authentication, hash function encryption, and digital signatures, etc..." | • Employ **strong and standard-based encryption protocol**s, such as the Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange.<br>• **Protect cryptographic keys** in FIPS-validated and tamper-evident hardware. | **Data Security**<br>Key Management<br>Hardware Security Modules |
| 2.2.8 "**Key management** should define a secure process covering the **creation and installation, storage and revoking of encryption keys**. | • **Centralize key lifecycle management** including generation, rotation, destruction, import and export.<br>• Manage encryption keys, provide **granular access control** and configure security policies.<br>• Ensure **secure deletion** by removing keys from CipherTrust Manager, digitally shredding all instances of the data.<br>• Support **cryptography algorithms** such as Advanced Encryption Standard (AES) 256bits, RSA 3072 bits.<br>• Offer **secure key exchange protocols** such as TLS/SSL (Mutual Authentication), PKCS#11, KMIP, REST API (over TLS), Elliptic Curve Diffie-Hellman (ECDH), Key Wrapping (AES-KW, RSA-KW).<br>• Provide **tight control to the HSM** with strong multi-factor authentication.<br>• **Protect cryptographic keys** in a FIPS 140-3 Level 3 environment.<br>• Easily **backup and duplicate sensitive cryptographic key** securely to the FIPS 140-3 Level3 certified backup HSM.<br>• Manage and protect all **secrets and sensitive credentials**. | **Data Security**<br>Hardware Security Modules<br>Key Management<br>Secrets Management |

| Description | How Thales helps | Thales Solutions |
|---|---|---|
| **2.3 Access Control** | | |
| "Enable **SSO to manage high-privilege accounts and user rights** effectively according to the principles of necessity of use and in accordance with the principles of good IT segregation of work, and to prevent unauthorized access..." | • Implement **Multi-Factor Authentication (MFA)** to ensure that only authorized individuals access the system.<br>• Deploy **Single Sign-On (SSO)** to allow users to securely access multiple systems with a single authentication.<br>• Set up access control policies based on user roles, responsibilities, and risks (**Adaptive Access Control**)<br>• Offer **audit system access** and store usage data (Access Logs) to support retrospective auditing. | **Identity & Access Management**<br>Adaptive Access Control<br>Delegated User Management<br>Multi-Factor Authentication<br>Single Sign-On (SSO) |
| **2.5 Communications Security** | | |
| 2.5.1 "Establish standards and procedures for data transmission via the organization's communication network and between the organization's internal communication network and external communication network ..." "...**guidelines to prevent unauthorized** changes, damage, or access to data, and there should be a **strict user verification process**..." | • Offer **Multi-Factor Authentication (MFA)** to prevent unauthorized network access.<br>• Create **network access** control policies based on user roles and risks.<br>• Offer **phishing-resistant authentication** (e.g., FIDO2 Security Keys, Certificate-Based Authentication) and restrict network access to authorized users only, based on trusted devices and verified identities. | **Identity & Access Management**<br>Adaptive Access Control<br>Multi-Factor Authentication |
| **2.6 IT Operations Security** | | |
| **2.6.4.1** "The event logs of the host, system, and important communication network devices are **stored in a secure manner**..." "...stored retrospectively for at least 90 days or as required by relevant laws..."<br>• Access log<br>• Important activity log, which must at least cover:<br>  ◦ Changes to the database structure and changes to data (update/insert/delete) in important tables<br>  ◦ Changes to system security settings<br>  ◦ Access to important system objects | • Monitor API activity, track usage, **detect anomalies**, and identify potential unauthorized access attempts.<br>• 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.<br>• Enforce **user rights management** based on data type and user role and produce reports for audit trails.<br>• **Capture detailed data activity** automatically for audit purposes.<br>• **Record all changes** to permissions, along with the identity of the perpetrator and session details. | **Application Security**<br>API Security<br><br>**Data Security**<br>Data Activity Monitoring<br>File Activity Monitoring<br><br>**Identity & Access Management**<br>Delegated User Management<br>Workforce Access Management |

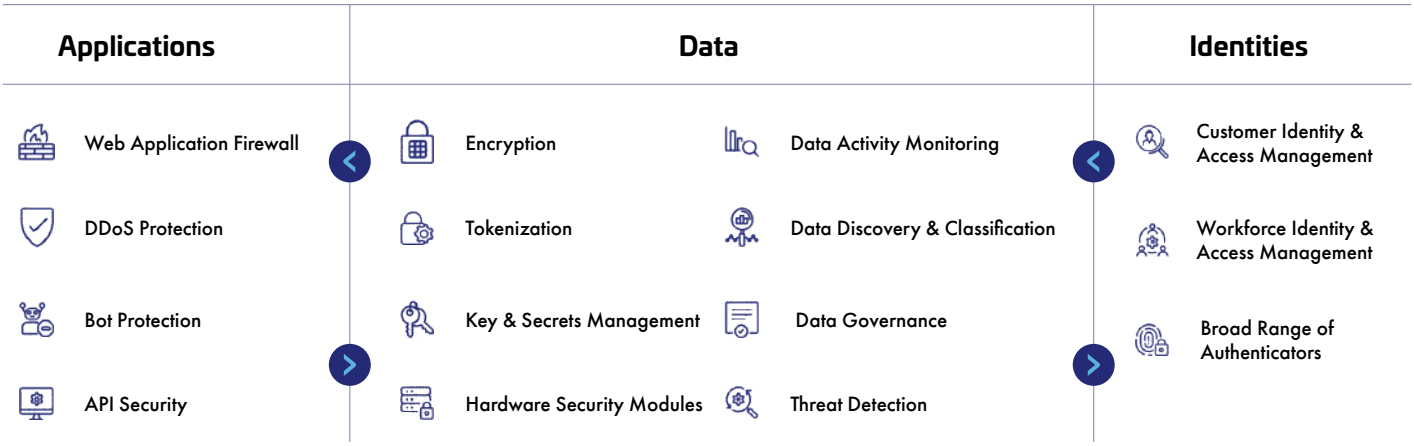
| Description | How Thales helps | Thales Solutions |
|---|---|---|
| **2.6.4.4** "Access logs and activity logs of IT personnel **with high privileges**, such as system administrators or system operators, are reviewed regularly..." | • **Adjust access permissions** based on real-time or near real-time user behavior and contextual factors.<br>• **Centralize access policies** and enforcement to multiple hybrid environments in a **single pane of glass**.<br>• Provide records of **access logs** and activities performed by privileged users (e.g., system administrators).<br>• Offer **records of audit logs** related to privilege usage for behavioral analysis and anomaly detection.<br>• - Provide **records of approval logs** related to privileged access requests and workflow execution. | **Identity & Access Management**<br>Delegated User Management<br>Multi-Factor Authentication<br>Single Sign-On (SSO)<br>Workforce Access Management |
| **2.6.6.2** "Establish processes or tools to promptly **detect abnormal events** that affect the security of critical systems, covering both physical and logical work systems and communication network systems..."<br>"...be aware of abnormalities or threats and be able to take **appropriate preventive or response** actions..." | • Monitor API activity, track usage, **detect anomalies**, and identify potential **unauthorized access attempts**.<br>• Safeguard critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic.<br>• Alert or block **database attacks and abnormal access** requests in real time.<br>• **Monitor file activity** over time to set up alerts on activity that can put financial institutions at risk.<br>• **Continuously monitor** processes for abnormal I/O activity and alerts or **blocks malicious activity**.<br>• 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.<br>• **Apply contextual security** measures based on risk scoring.<br>• **Centralize access policies and enforcement** to multiple hybrid environments in a single pane of glass.<br>• **Build and deploy adaptive authentication** policies based on the sensitivity of the data/application.<br>• **Monitor user behavior** such as admin login from a new location/IP or a wrong system access pattern to alert and prevent attack.<br>• **Analyze User Behavior Analytics (UBA) and context** such as time/device/network to add authentication or block access. | **Application Security**<br>API Security<br>Bot Protection<br>DDoS Protection<br><br>**Data Security**<br>Data Activity Monitoring<br>File Activity Monitoring<br>Transparent Encryption<br>Ransomware Protection<br><br>**Identity & Access Management**<br>Adaptive Access Control<br>Fraud & Risk Management<br>Multi-Factor Authentication<br>Workforce Access Management |
| **2.6.7 Vulnerability Management and Penetration Test** | | |
| **2.6.7.2** "...processes and tools for **vulnerability assessment**. Financial institutions and specialized financial institutions should determine the scope and frequency of vulnerability assessment to cover all systems consistently according to the risk level..." | • Offer **advanced API Verification capabilities** to strengthen your defenses against potential vulnerabilities.<br>• Run **assessment tests** on data stores such as MySQL or so to scan for known vulnerabilities.<br>• **Scan your databases** with over 1,500 predefined vulnerability tests based on CIS and PCI-DSS benchmarks to help you keep your databases covered for the latest threats. | **Application Security**<br>API Security<br><br>**Data Security**<br>Data Activity Monitoring<br>File Activity Monitoring |

| Description | How Thales helps | Thales Solutions |
|---|---|---|
| **2.6.9 Endpoint Security** | | |
| **2.6.9.1** "Establish **written standards and procedures** for security of equipment used for work, both for the **SSO** and personal devices (Bring Your Own Device: **BYOD**) ..."<br><br>**2.6.9.2** "Establish a Security **Baseline for the SSO's** equipment used for work ..."<br><br>**2.6.9.3** Have a process for **managing** personal devices (Bring Your Own Device: **BYOD**), from registration, renewal, and cancellation of BYOD use. | • Manage system access from both corporate and BYOD devices with **Identity Verification and Multi-Factor Authentication (MFA)**.<br>• Enforce **contextual access policies** and **control system** and **data access rights** based on device and user role risks, such as denying access from unregistered or high-risk devices.<br>• **Verify device identities** with digital certificates or trusted authorities before allowing connections. | **Identity & Access Management**<br>Adaptive Access Control<br>Identity Verification<br>Multi-Factor Authentication |
| **2.7 System Acquisition and Development** | | |
| **2.7.2.17** "...guidelines for controlling the security and confidentiality of important data used in testing, such as **data masking**, to **prevent the risk** of leakage of such important data..." | • **Pseudonymize sensitive information** in databases to prevent exposure of real data for testing. | **Data Security**<br>Tokenization |
| **2.10 Third Party Management** | | |
| 2.10.1 "...applying the Bank of Thailand's implementation guidelines on third-party risk management as guidelines for **managing external risks** appropriately and in accordance with the scope, risk level and significance of using services, connecting to or accessing information from external parties..." | • **Manage the identity of external service providers** by checking and verifying their identities before granting access to systems or sensitive data.<br>• **Enforce access policies** based on role and risk of the provider to limit access to only the necessary scope of work.<br>• **Manage access rights** and assign management rights to administrators or supervisors.<br>• **Track and store logs** of external service provider access activities to support retrospective auditing. | **Identity & Access Management**<br>Adaptive Access Control<br>Delegated User Management<br>Fraud & Risk Management<br>Identity Verification |

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.