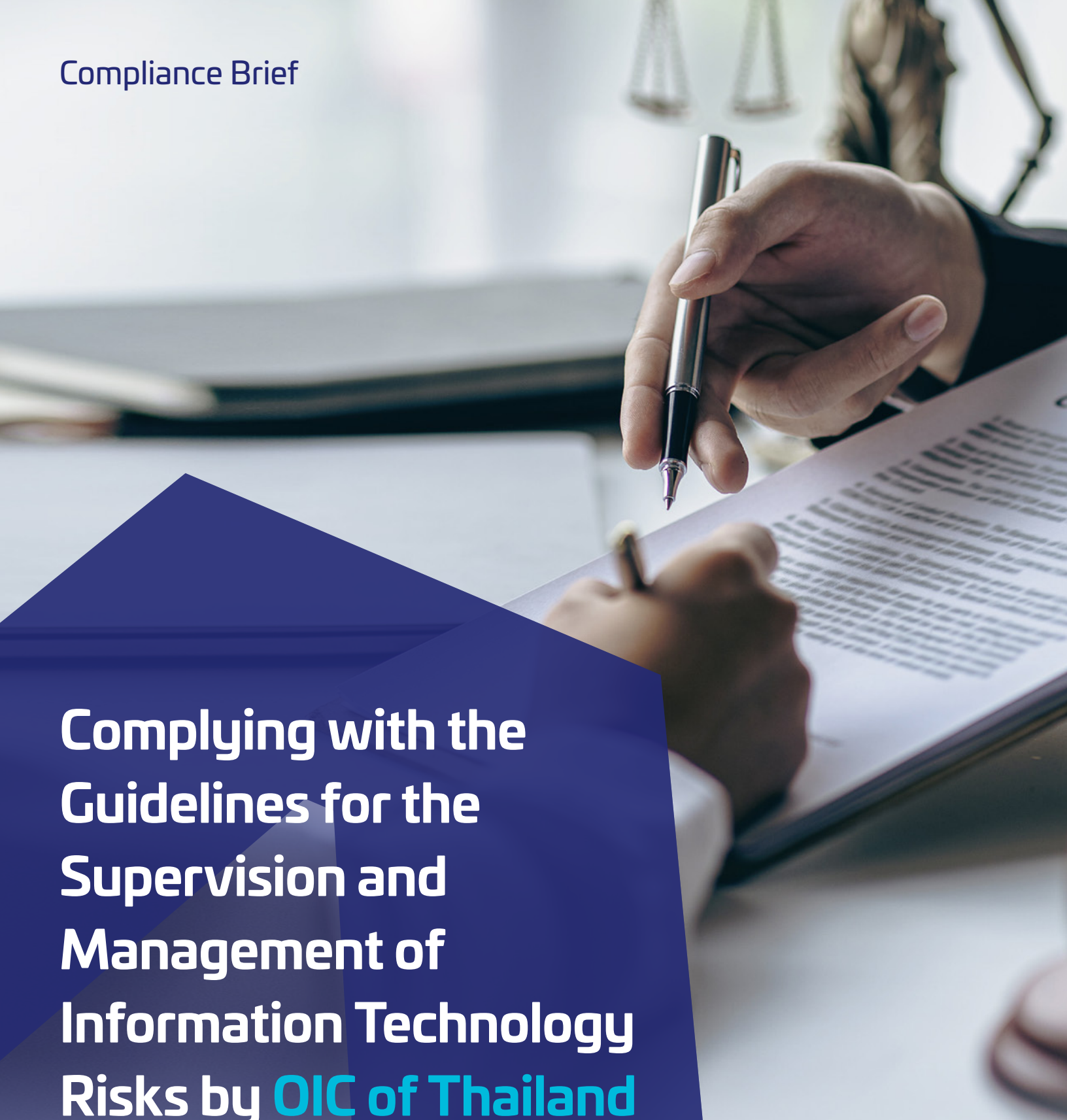
Compliance Brief



Complying with the Guidelines for the Supervision and Management of Information Technology Risks by OIC of Thailand

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

The Guidelines for the Supervision and Management of Information Technology Risks of Life Insurance Companies B.E. 2563 (2020) (หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสน เทศของบริษัทประกันชีวิต พ.ศ. ๒๕๖๓) were issued by the Office of Insurance Commission (OIC) of Thailand to strengthen IT risk management in the life insurance sector.

What are the Guidelines for the Supervision and Management of Information Technology Risks by OIC?

1. Purpose:

- Ensure secure and stable IT operations in life insurance companies
- Mitigate risks from cyber threats, data breaches, and system failures
- Align with international standards
- Enhance regulatory compliance and consumer protection

2. Scope:

- All life insurance companies registered in Thailand
- Third-party service providers (handling IT systems/data for insurers)

3. Guidelines:

- 6 categories: IT Governance, IT Project Management, IT Security, IT Risk Management, IT Compliance, IT Audit, Cybersecurity Governance and Risk Management and Reporting of Cyber Threat Incidents.

How Thales Helps with the OIC – Guidelines for the Supervision and Management of Information Technology Risks

Thales' solutions can help organizations address 2 categories – IT Security and Cybersecurity Governance and Risk Management by simplifying compliance and automating security with visibility and control, reducing the burden on security and compliance teams.

Description	How Thales helps	Thales Solutions
IT Security		
Article 16 "... provide **information asset** management, which must include at least the following:" (2) "Must provide appropriate information classification practices according to the level of confidentiality and importance of the organization's information, and must establish security guidelines that are consistent with the level of confidentiality..."	• **Identify** structured and unstructured **sensitive data** at risk across Hybrid IT. • Identify the current state of **compliance and document gaps**. • **Discover and classify** potential risk for all public, private and shadow APIs. • 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.	**Application Security** API Security **Data Security** Data Discovery & Classification

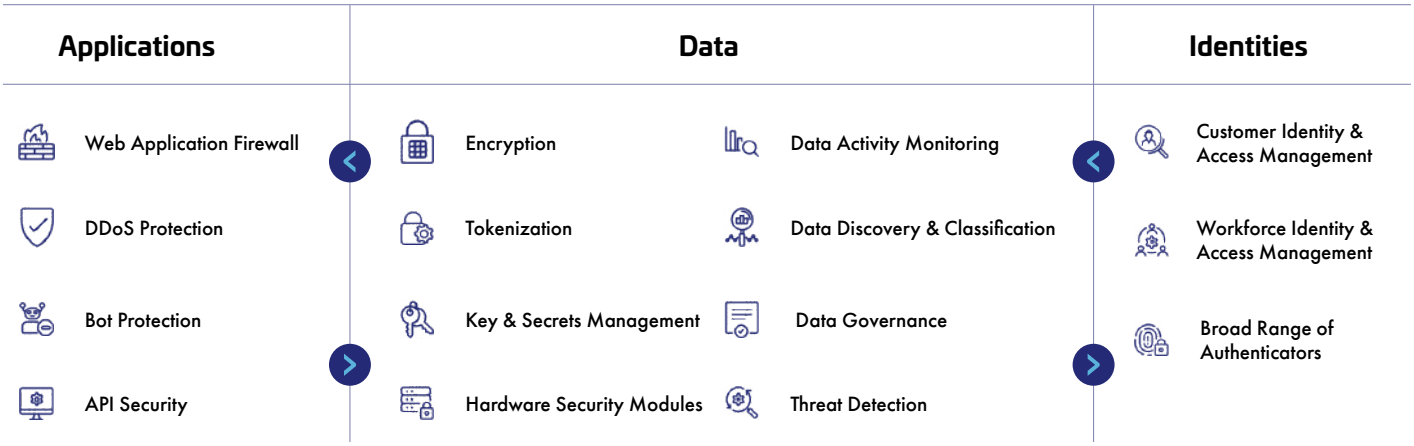
Description	How Thales helps	Thales Solutions
Article 17 "... provide **access control** to the system, data, and information assets to prevent unauthorized or unauthorized access to and modification of the system or data, which must include at least the following:" 1) "Establish **a policy for access** to or use of the system, data, and information technology assets..." 2) "Establish **management of user rights and verification of identity** according to the specified rights..." 3) "Establish review and improvement of user rights..." 4) "Establish **revocation of user rights** when there is a change in job duties or termination of employment..."	• **Limit the access** of internal and external users to systems and data based on **roles and context** with policies. • Apply contextual security measures based on **risk scoring**. • **Centralize access policies** and enforcement to multiple hybrid environments in a single pane of glass. • **Unify key managemen**t operations with role-based access control. • **Offer Multi-Factor Authentication (MFA)** to ensure that those accessing the system are truly authorized. • Employ Single **Sign-On (SSO)** to allow users to securely access multiple systems with a single authentication. • Set up **access policies** based on user roles, responsibilities, and risks.	**Application Security** API Security **Data Security** Data Activity Monitoring File Activity Monitoring Key Management Transparent Encryption **Identity & Access Management** Adaptive Access Control Multi-Factor Authentication Single Sign-On (SSO)
Article 18 "...maintain a **cryptography practice** to ensure the security of information appropriately, according to the **level of confidentiality and importance of the information...**"	• Deploy **transparent and continuous encryption** that protects against unauthorized access by users and processes in physical, virtual, and cloud environments. • **Pseudonymize sensitive information** in databases to prevent exposure of real data for testing. • **Protect cryptographic keys** in FIPS 140-3 Level 3 and tamper-evident hardware. • Encrypt Keys with a one-time-use **AES 256 key** and send over a mutually authenticated **TLS connection**. • Security products designed for **post-quantum** upgrade to maintain crypto-agility.	**Data Security** Hardware Security Modules Key Management Tokenization Transparent Encryption
Article 20 "... have a network and communication security system, which shall be implemented at least as follows:" (2) "The Company shall have **control and limitation of remote access** rights to the network and information systems..."	• **Enable Multi-Factor Authentication (MFA)** for remote users to ensure that access is authorized. • Provide **user rights management** for the Virtual Private Network (VPN) system to prevent access from unauthorized devices. • Offer **Remote Access Policies** control users.	**Identity & Access Management** Adaptive Access Control Multi-Factor Authentication Risk-Based Authentication

Description	How Thales helps	Thales Solutions
Article 21 (6) Arrange for system monitoring and threat surveillance **(security monitoring)** by having processes or tools to **detect unusual events or threats** that affect the security of important systems, including managing system vulnerabilities (**vulnerability management**)..." "...especially **application systems and networks** that are connected to public communication networks (internet facing) ..."	• **Detect and prevent cyber threats** with a 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. • 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. • Offer **transparency and context into your data risk** status by consolidating data risk metrics, locating risk areas, and providing transparent and customizable risk scores.	**Application Security** API Security Attack Analytic Bot Protection DDoS Protection Web Application Firewall **Data Security** Data Activity Monitoring Data Risk Analytics Data Risk Intelligence File Activity Monitoring
Cybersecurity Risk Governance and Management		
Article 39 "... conduct inspection and monitoring of cyber threats (detection) by taking at least the following actions:" (2) "Establish guidelines for searching, testing and managing information technology vulnerabilities in order to detect, analyze, track and notify unusual events or cyber threats to the departments or responsible persons..."	• **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

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.

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.

© Thales - August 2025 • EHv6