

Complying with the Bank of Thailand (BOT) AI Risk Management Guidelines

The Bank of Thailand (BOT) issued Policy Guideline No. BOT.3.5994/2568 on [Risk Management for the Use of Artificial Intelligence Systems](#). The guideline provides a framework for financial institutions to identify, manage, and monitor the risks associated with the use of AI.

What are the BOT AI Risk Management Guidelines?

AI can improve efficiency, decision-making, and customer experience, but it also introduces risks such as inaccurate results, bias, poor data quality, and cybersecurity threats. The **BOT AI Risk Management Guidelines** help financial institutions use AI responsibly by establishing clear governance, oversight, and risk management practices. It covers two main areas:

- **AI Governance:** defining the roles and responsibilities of boards and senior management.
- **AI Development and Security Controls:** managing risks throughout the AI lifecycle, including data, models, monitoring, and security.

Objectives

The **BOT AI Risk Management Guidelines** help financial institutions:

- Apply risk management based on the level of AI risk and business impact.
- Use AI in line with the **FEAT principles** of Fairness, Ethics, Accountability, and Transparency.
- Work alongside existing BOT requirements for IT risk, cybersecurity, data governance, and consumer protection.

Risk Management Principles for Using AI Systems

The BOT guidelines state that financial institutions should:

1. Remain accountable for the use of AI systems and their outcomes.
2. Apply the FEAT principles when developing and using AI.
3. Manage risks throughout the entire AI lifecycle.
4. Protect customers through transparent and fair AI practices.

How Thales Helps with BOT AI Risk Management Guidelines Compliance

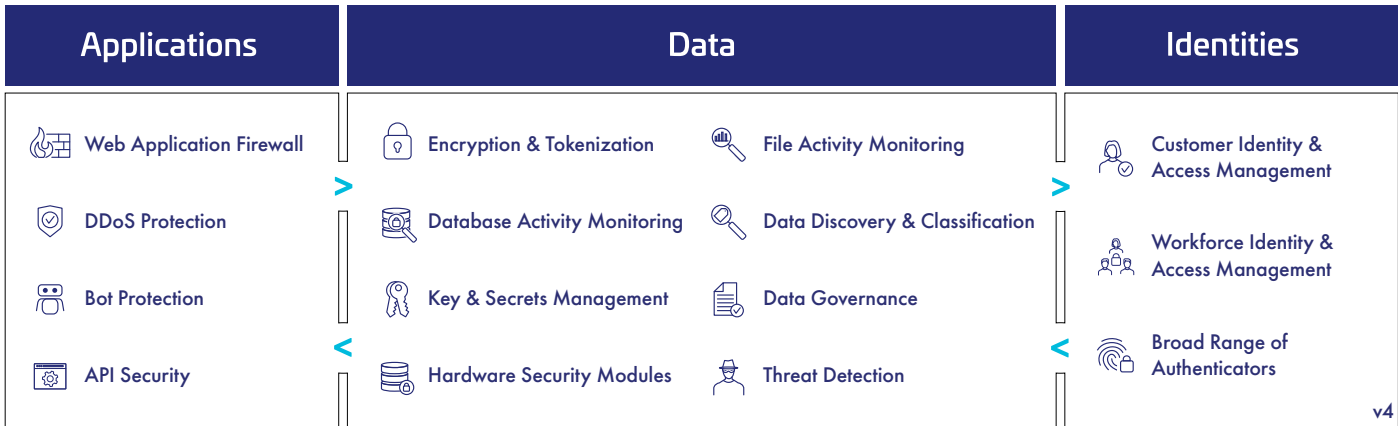
Thales helps financial institutions in Thailand align with the Data Risks, Model Development and Cybersecurity Controls of the AI Development and Security Controls in the Guidelines.

AI Development and Security Controls	How Thales Helps	Solution Areas
Data Risk Controls		
• Quality Metrics • Data Cleansing	• Integrate generative machine learning into its discovery engine to understand semantic context. • Automatically crawl, identify, and catalog data pools across hybrid clouds and on-premises environments before feeding bulk data into an LLM or credit-scoring model. This enables data compliance teams to audit the integrity and diversity of training sets before model ingestion.	Data Security • Data Discovery & Classification

AI Development and Security Controls	How Thales Helps	Solution Areas
Data Leakage Defenses	- Provide Static and Dynamic Data Masking along with Vaultless Tokenization. When sensitive data (such as customer PII or account numbers) is passed to an AI model or commercial chatbot, dynamic masking replaces the sensitive data with tokens or masked hashes in real time. - Transparently intercept RESTful API calls destined for third-party AI models (e.g., OpenAI or external LLMs) and sanitize the input by stripping or encrypting sensitive values before the text crosses the corporate data boundary.	Data Security Batch Data Transformation Data Protection Gateway Tokenization
Model Development Controls		
- Performance Metrics - Stress Testing	- Provide FIPS 140-2 Level 3 cryptographic security to anchor the cryptographic keys used to sign and lock AI model binaries, as the root of trust for any AI model relies on the integrity of its code and execution parameters. - Ensure that once an AI model is verified and deployed, its mathematical weights cannot be subtly altered or tampered with by an insider or malicious actor.	Data Security Hardware Security Modules
- Generative AI Guardrails - Explainability Documentation	- Address runtime security for agentic AI and LLMs, the AI Security Fabric serves as a specialized proxy layer between users, enterprise RAG applications, and foundation models. Audit the interaction flow and help compliance teams trace exactly how inputs correlate to outputs. - Provide detailed, auditable file and database access logs that record exactly who, what process, and when an AI engine accesses proprietary corporate knowledge bases. This generates the absolute paper trail required by BOT auditors to evaluate algorithmic transparency and data lineage.	Data Security AI Security Fabric Security Intelligence
Cybersecurity Controls		
- Content Filtering - Vulnerability Testing	Detect and block malicious prompts in real-time, and prevent leakage of sensitive information from responses. Detect anomalies associated with Adversarial Attacks (manipulated structural payloads) and strip away malicious inputs before they can trigger logic flaws in the neural network. Inspect API traffic entering AI orchestration layers. - Isolate legitimate traffic from malicious automated actors and mitigate high-frequency bot injection vectors.	Application Security AI Application Security API Protection Web Application Firewall Bot Protection
Threat Intelligence Tracking	Build baseline profiles of normal user and machine behavioral patterns. By mapping behavioral anomalies against the OWASP Top 10 for LLM Applications and MITRE ATLAS parameters, the platform flags indicators of compromise – as automated Model Inversion attempts – before systemic extraction occurs.	Data Security Data Risk Analytics

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.

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.