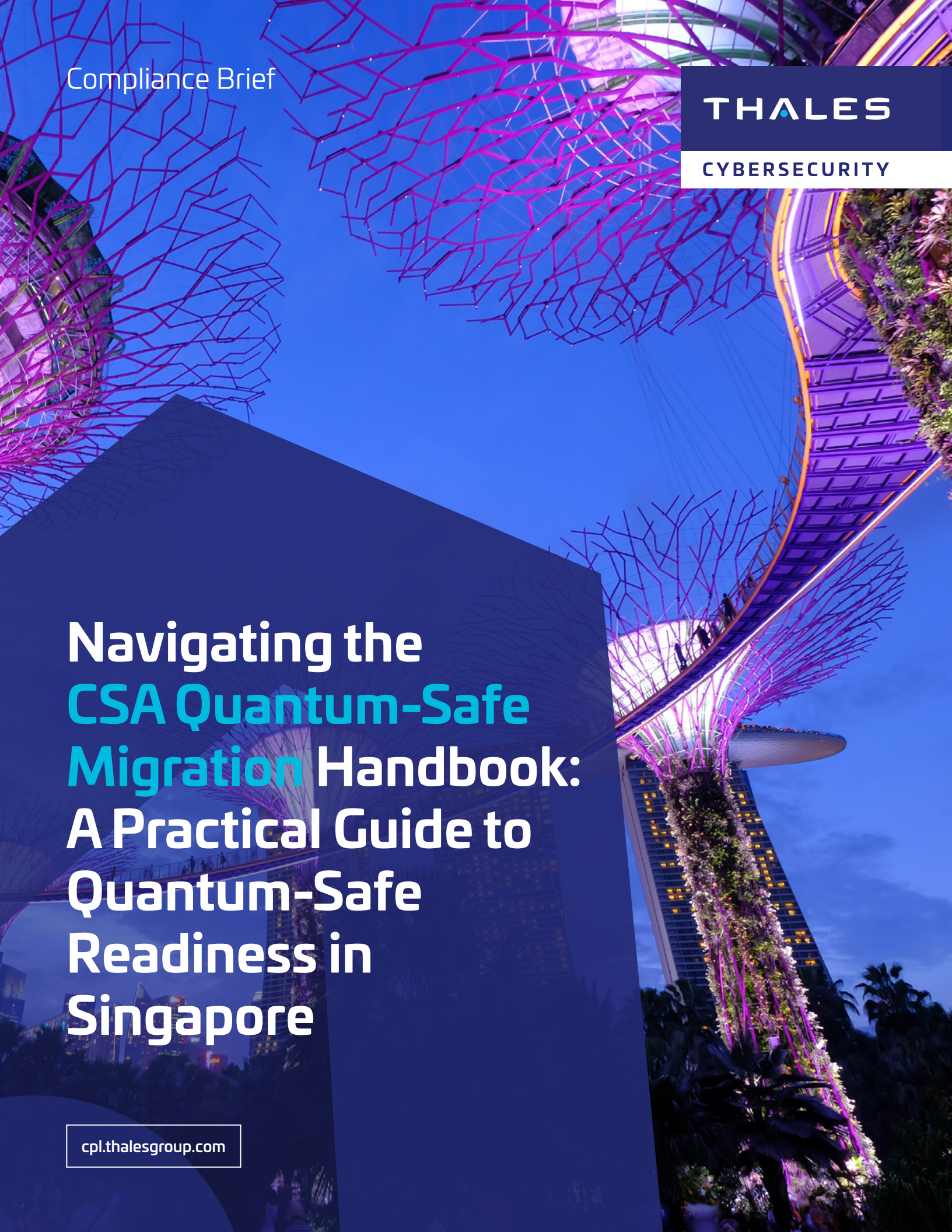
Compliance Brief

THALES

CYBERSECURITY



Navigating the CSA Quantum-Safe Migration Handbook: A Practical Guide to Quantum-Safe Readiness in Singapore

cpl.thalesgroup.com

THALES

CYBERSECURITY

Cyber Security Agency of Singapore (CSA) introduced the Quantum-Safe Migration Handbook and the Quantum Readiness Index (QRI) as complementary resources to help organizations prepare for the transition to quantum-safe cryptography on July 16, 2026.

As quantum computing advances, today's widely used public-key cryptography, such as RSA and ECC, will become increasingly vulnerable. The Quantum-Safe Migration Handbook provides practical guidance for planning and implementing a phased migration to post-quantum cryptography (PQC), while the QRI enables organizations to assess their readiness, identify capability gaps, and prioritize next steps.

What is the Quantum-Safe Migration Handbook?

The **Quantum-Safe Migration Handbook**, published by the Cyber Security Agency of Singapore (CSA) in collaboration with GovTech, IMDA, and industry partners, helps organizations prepare for the transition to quantum-safe cryptography. It provides practical guidance across five domains to assess quantum risks, identify cryptographic assets, build crypto agility, plan a phased migration to post-quantum cryptography (PQC), and adapt to evolving technologies and standards.

Which organizations need to align with this handbook?

The handbook serves as a broad national reference; adoption falls into two categories: **mandatory/regulated entities** with strict national deadlines, and **organizations strongly advised to align** due to high risk.

Categories	Organizations

Mandatory & Regulated Entities (Strict Compliance)	**Critical Information Infrastructure (CII) Owners:** Organizations operating essential services across **11 critical sectors:** Banking & Finance, Energy, Healthcare, Info-communications, Water, Transportation, Government, Emergency Services.
	• **Mandatory Milestones:**
	  ◦ **March 2027:** Summit comprehensive quantum-safe migration plans to CSA
	  ◦ **2028 – 2031:** Ensure all new digital systems support quantum-safe tech starting in 2028, and complete full migration by end of 2031.

	• **Government Ministries & Public Sector Agencies:** Agencies managing public data, citizen portals, digital identity platforms (e.g., Singpass), and core civil service infrastructure (guided in tandem by GovTech).
High-Priority Organizations (Strongly Advised to Align)	• **Financial Institutions & FinTech:** Entities managing long-term financial records and cross-border transactions aligned with MAS cyber-resilience rules. • **Long-Shelf-Life Data Custodians:** Organizations holding IP, biometrics, trade secrets, or health data vulnerable to "Harvest Now, Decrypt Later" attacks. • **Telcos & Cloud Service Providers:** IMDA-regulated infrastructure providers hosting and securing enterprise and government network transit. • **IT Vendors & System Integrators:** Software and hardware suppliers required to meet upcoming procurement mandates for post-quantum compatibility and cryptographic agility.

How Thales Helps with The Quantum-Safe Migration Handbook in Singapore?

Thales's solutions together with Professional Services help organizations align with the CSA Quantum-Safe Migration Handbook by providing expert advisory, cryptographic assessments, migration planning, and trusted security solutions that accelerate quantum-safe readiness, strengthen cryptographic governance, and execute a structured transition to crypto-agile environments.

Thales **Professional Services** guides organizations through every stage of their quantum-safe journey – from planning and readiness assessment to migration and governance – helping them build a risk-based roadmap, strengthen cryptographic governance, and achieve long-term crypto agility.

Phase 1 – Planning

- Establish governance structures, roles, responsibilities, and RACI models.
- Develop a quantum-safe roadmap aligned with CSA requirements.
- Support preparation of the migration plan for approval and submission.
- Leverage the Thales PQC Migration Framework to assess risks and plan migration, including:
  - Perform Risk Assessment for ciritical applications based on impact and Mosca scores
  - Adopt threat modeling to prioritize critical systems.

Phase 2 – Discovery & Assessment

- Build a cryptographic inventory and CBOM for critical systems.
- Assess quantum risks and measure readiness against relevant QRI domains.
- Identify capability gaps and create a prioritized roadmap toward crypto agility.
  - Migrate from TLS 1.2 to TLS 1.3 to enable PQC for critical systems.
  - Protect sensitive data at rest with AES-256 for critical systems.

Phase 3 – Migration & Governance Execution

- Execute migration based on approved risk priorities.
- Adopt quantum-safe/ hybrid certificates.
- Implement governance for cryptographic and key management changes.
- Track progress, manage remediation, and support modernization across cryptographic infrastructure.

Thales's Solutions support organizations across three domains of the CSA Quantum-Safe Migration Handbook by providing centralized visibility of cryptographic assets, trusted key and data protection, and crypto-agile security solutions that simplify cryptographic management, strengthen governance, and reduce operational risk.

Domain 1: Risk Assessment

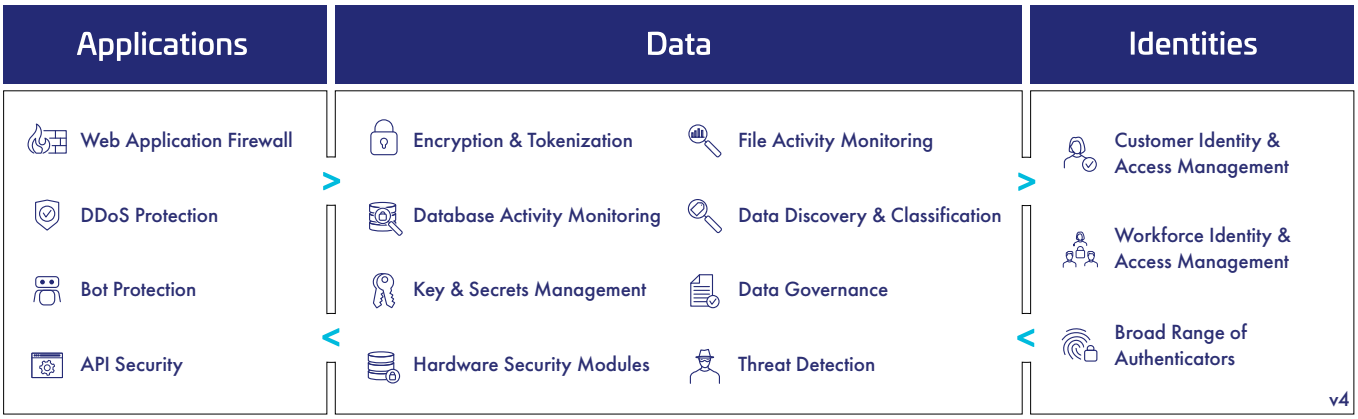
• Identify critical systems • Prioritise migration	• Identify crown jewel applications and high-value information assets requiring priority protection. • Provide visibility into where sensitive data is stored and protected, helping organizations focus migration on the systems with the greatest business impact.	**Data Security** Data Discovery & Classification Data Risk Analytics File Activity Monitoring
• Build a cryptographic inventory	• Build a cryptographic inventory using existing documentation, PKI records, HSM logs, and key management systems. • Gain centralized visibility into managed cryptographic assets—including encryption keys, certificates, HSMs, and cryptographic policies. • Supplement with ACDI tools to discover cryptographic assets across applications, networks, and endpoints. • Keep the cryptographic inventory up to date to support ongoing migration and crypto-agility.	**Data Security** Hardware Security Modules Cloud Key Management Key Management

Domain 1: Risk Assessment		
• Protect high-value data • Reduce interim risk • Support risk reporting	• Protect high-value data with AES-256 encryption, tokenization, application data protection, and HSM-backed key security. • Secure long-term confidential data (financial records, healthcare data, PII, intellectual property) that the handbook identifies as high-priority targets for Harvest-Now, Decrypt-Later attacks. • Enforce strong encryption (for example, AES-256), centralized key management, and least-privilege access controls to reduce current risk before full PQC migration. • Support security teams in understanding which assets are protected and demonstrate progress during migration planning with centralized auditing and reporting.	**Data Security** Application Data Protection Hardware Security Modules Cloud Key Management Key Management Secrets Management Tokenization Transparent Encryption
Domain 2: Governance		
• Governance and accountability • Cryptographic inventory • Cryptographic policy enforcement • Key lifecycle management	• Establish cryptographic governance with centralized management of keys, policies, and cryptographic assets, role-based administration, and separation of duties. • Maintain a live cryptographic inventory with visibility into encryption keys, encryption policies, HSMs, and protected assets. • Maintain cryptographic policies with centralized policy management for encryption, key usage, rotation, separation of duties, and access control • Offer automated generation, rotation, backup, archival, revocation, expiration, and destruction of keys.	**Data Security** Cloud Key Management Hardware Security Modules Key Management Secrets Management
• Support procurement and technology refresh • Crypto-agility	• Simplify adoption of quantum-safe technologies and future algorithm transitions with standards-based cryptographic infrastructure (KMIP, PKCS#11, REST APIs). • Integrate NIST-standardized algorithms like ML-KEM, ML-DSA, and SLH-DSA into commercial encryption platforms, smartcards, and high-assurance hardware.	**Data Security** Hardware Security Modules
• Monitoring and reporting • Hybrid enterprise governance	• Provide comprehensive audit logs, key usage tracking, compliance reporting, and SIEM integration • Offer third-party, cloud governance and unified key management across on-premises, cloud, and hybrid environments.	**Data Security** Cloud Key Management Key Management Secrets Management
Domain 3: Technology		
Cryptographic key protection	• Provide FIPS-certified hardware protection for cryptographic keys and root of trust.	**Data Security** Hardware Security Modules
Centralized key lifecycle management	• Offer centralized management of key generation, rotation, backup, revocation, destruction, auditing, and policy enforcement.	**Data Security** Cloud Key Management Key Management
Data-at-rest protection	• Protect sensitive data using strong encryption such as AES-256	**Data Security** Application Data Protection Tokenization Transparent Encryption
PKI modernization	• Secure Certificate Authority (CA) private keys and support modernization toward PQC-enabled PKI architectures.	**Data Security** Hardware Security Modules

Domain 3: Technology		
Crypto agility	• Centralize cryptographic policies and key management, making algorithm transitions easier.	**Data Security** Cloud Key Management Key Management
Hybrid migration	• Support coexistence of classical and emerging PQC implementations during transition with HSM and PKI infrastructure.	**Data Security** Hardware Security Modules
Secure application integration and DevSecOps	• Enable applications to adopt new cryptographic services with minimal code changes. • Offer APIs and automation to integrate key management into CI/CD pipelines and cloud-native deployments.	**Data Security** Cloud Key Management Key Management RESTful API Secrets Management
• Enterprise-wide governance • Validate and audit	• Provide centralized visibility into encryption keys, policies, and protected assets. • Support validation through FIPS-certified HSMs, audit logging and policy enforcement.	**Data Security** Cloud Key Management Hardware Security Modules Key Management Secrets Management

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.