cpl.thalesgroup.com

THALES
Building a future we can all trust

Complying to Secure Tertiary Data Backup (STDB) Guideline in Hong Kong

Destructive malware, including ransomware, is of growing concern as it can potentially lead to permanent loss, corruption or unauthorized alteration of critical data in both production and backup environments. In light of recent international developments such as the U.S. Sheltered Harbor initiative to address this type of cyber threat, the Hong Kong Monetary Authority (HKMA) has invited the Hong Kong Association of Banks (HKAB) to develop guidelines on Secure Tertiary Data Backup (STDB) that are appropriate for the banking landscape in Hong Kong on April 30, 2021.

What is Secure Tertiary Data Backup (STDB) Guideline?

The **Secure Tertiary Data Backup (STDB)** Guideline is an industry standard for the banking sector on data protection, portability, recovery and the continuity of critical services. It provides guidance to banks on the factors they need to take into account in deciding whether to set up an STDB and what implementation issues they need to overcome in ensuring the effectiveness of the STDB.

The Guideline covers the eight high-level **Principles** and embeds with nine **Data Vault Characteristics** under the headings of Governance, Design and Data Restoration. The HKMA considers STDB an effective measure to enhance the cyber resilience and data security of Authorized Institutions (AIs) in Hong Kong. It expects all AIs to critically assess the need for implementing an STDB having regard to their risk exposure and taking into account the principles stipulated in the HKAB's STDB Guideline.

Principles	Data Vault Characteristics
1. STDB Governance Model	1. Immutable
2. Identification of Critical Data	2. Survivable
3. Data Quality	3. Air-gapped
4. Critical Data Lifecycle Management	4. Secure
5. Data Extraction and Ingestion	5. Controlled
6. Secure Repository	6. Verifiable
7. Restoration Planning	7. Assurance
8. Restoration Validation Process and Drills	8. Heterogeneous
	9. High-performance

How can Thales help?

As the leader in digital security and data protection, Thales has helped hundreds of enterprises comply with regulations worldwide by recommending the appropriate data protection technologies required to meet regulatory requirements.

Thales enables Authorized Institutions (AIs) to align with the key principles in the Secure Tertiary Data Backup (STDB).

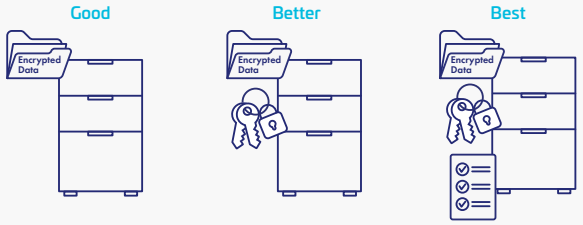
Simplify Data Security

Discover, protect, and control your organization's most sensitive data on-premises and in the cloud on an integrated data security platform.

Accelerate Time to Compliance

Comprehensive data security capabilities, including data discovery and classification, encryption, granular access controls, audit logs, tokenization, and key management support ubiquitous data security and privacy.

Best practices to protect the Critical Data



Self-Encrypting Storage

Data Storage Systems utilize self-encrypting disks to protect data at rest.

If the cybercriminal finds the key then the data is open to be viewed.

Self-Encrypting Storage + Key Management

While Data Storage Systems utilize self-encrypting disks to protect data, the Key Manager protects the key that unlocks the data.

The key is not well protected and managed with market-standard solutions.

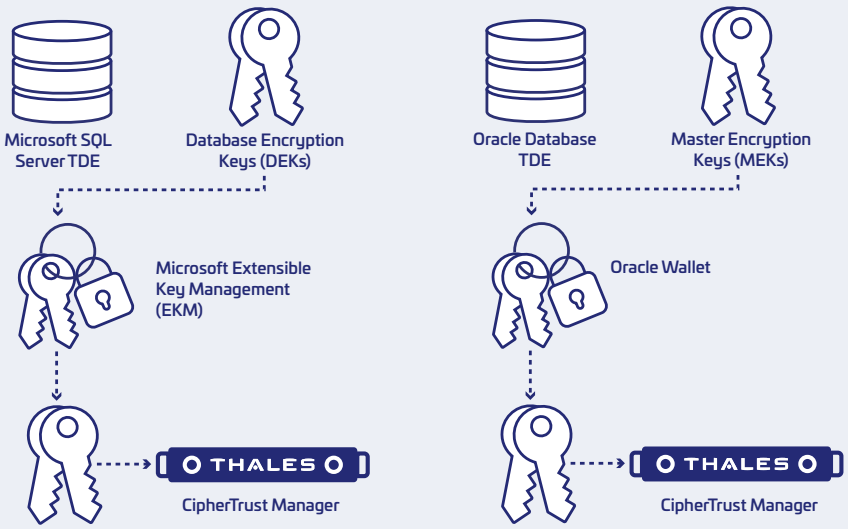
Self-Encrypting Storage + Key Management + Access Control

Data Storage Systems utilize self-encrypting disks to protect data, while the Key Manager protects the key and transparent encryption ensures that only valid users see the data.

Users and applications must be validated to access viewable data.

Principles	Thales Solution
1. STDB Governance Model: • Authorized Institutions (AIs) should conduct a risk assessment to determine the need to implement the STDB. AIs should have controls in place to provide reasonable assurance that there is effective governance and management supervision of their STDB activities. • Policies, standards and procedures should be established for all relevant control areas, including but not limited to data quality, data completeness, data access, authorized use, entitlement control, data privacy, data security and data description.	**Segregation of duties, access control, audit log and reporting** Thales enables AIs to achieve segregation of duties, access control, log and reporting. • CipherTrust Manager enhances key management by delivering a **strong separation of duties** for increased security. It offers multi-tenancy, or domains, allowing customers and service providers to generate unique key management environments. This provides additional security and ultimate separation of duties, where no single administrator has access to all domains. Additionally, CipherTrust Manager enforces very granular and least-privileged-user access management policies, enabling the protection of data from misuse by privileged users. Granular privileged-user-access management policies can be applied by user, process, file type, time of day, and other parameters. • **Access logs and reporting:** CipherTrust Security intelligence of the CipherTrust Data Security Platform provides Security Intelligence logs that specify which processes and users have accessed protected data, under which policies, and if access requests were allowed or denied. • The management logs will even expose when a privileged user submits a command such as 'switch users' to imitate, and potentially exploit, the credentials of another user. Sharing these logs with a security information and event management (SIEM) platform helps uncover anomalous patterns in processes and user access, which can prompt further investigation.
2. Identification of Critical Data: AIs should **establish the scope of their critical data** with reference to those of their functions, services and systems that are **most critical** (these could include both internal and outsourced systems that are considered essential to the AI and the banking ecosystem, or could encompass application objects and document objects if applicable). AIs should regularly evaluate whether the scope of their critical data needs to be revised by reviewing existing and/or ongoing business impact assessments of their critical functions, services and systems.	**Establishing the scope of their critical data** Thales' CipherTrust Data Discovery and Classification efficiently identifies structured as well as unstructured sensitive data on-premises and in the cloud for the AIs. • Supporting both agentless and agent-based deployment models, the solution provides built-in templates that enable rapid identification of regulated data, highlight security risks, and help you uncover compliance gaps. A streamlined workflow exposes security blind spots and reduces remediation time. Detailed reporting supports compliance programs and facilitates executive communication.

Principles	Thales Solution
4. Critical Data Lifecycle Management: AIs should design and implement controls to securely store, validate and manage critical data throughout its lifecycle. • Critical data should undergo **both in-transit and at-rest encryption**. Tools and processes to prevent and/or detect unauthorized access to, or exfiltration of, critical data should be applied. • Critical data should only be usable by parties who are authorized for specific STDB activities (e.g. viewing, updating, sharing, relocating, etc.).	**Protecting critical data in transit and at rest with encryption** CipherTrust Transparent Encryption (CTE) delivers **data-at-rest encryption** with centralized key management, privileged user access control and detailed data access audit logging. • Protect data wherever it resides, on-premises, across multiple clouds and within big data, and container environments. • Work in conjunction with the FIPS 140-2 up to Level 3 compliant CipherTrust Manager, which centralizes encryption key and policy management for the CipherTrust Data Security Platform. Thales High Speed Encryptors (HSEs) provide network-independent data-in-transit encryption (Layers 2, 3 and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. • Allow organizations to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception—all at an affordable cost and without performance compromise.

5. Data Extraction and Ingestion:
 	
AIs should implement controls to provide reasonable assurance that throughout the data extraction and ingestion processes, critical data is encrypted in accordance with industry good practices and transmitted completely and accurately on a regular basis.
 	
• Critical data should undergo both **in-transit and at-rest encryption**. Tools and processes to prevent and/or detect unauthorised access to, or exfiltration of, critical data should be applied.
• Critical data should only be usable by parties who are authorised for specific STDB activities (e.g. viewing, updating, sharing, relocating, etc.).
	Key Management & key lifecycle management
	
	CipherTrust Manager simplifies key lifecycle management tasks, including secure key generation, backup/restore, clustering, deactivation, and deletion by enabling organizations to centrally manage encryption keys for Thales CipherTrust Data Security Platform and third-party products —including IBM Security Guardium Data Encryption, Microsoft SQL TDE, Oracle TDE, and KMIP-compliant encryption products.
	
	• By consolidating key management, it fosters consistent policy implementation across multiple systems and reduces training and maintenance costs. Or, use standards-based APIs, to simplify the deployment of applications integrated with key management capabilities and automate testing and development of administrative operations.
	• CipherTrust Manager offers the following Enterprise Key Management solutions.
	  ◦ CipherTrust KMIP Clients: Centrally manage keys across a variety of KMIP clients.
	  ◦ CipherTrust LUKS Agents: provides transparent data encryption on Linux servers using Linux Unified Key Setup (LUKS) Agents.
	  ◦ CipherTrust **Transparent Database Encryption (TDE)** Key Agents: Protects data in databases using Transparent Data Encryption (TDE) Key Agents on Oracle and Microsoft SQL Servers.
	
	 
	
	(Continue on page 4)

Principles	Thales Solution

5. Data Extraction and Ingestion	**Protection of cryptographic keys**
	Luna HSMs from Thales provide a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more.
	• Available in three FIPS 140-2 certified form factors, Luna HSMs support a variety of deployment scenarios.
	• In addition, Luna HSMs:
	  ◦ Generate and protect root and certificate authority (CA) keys, providing support for PKIs across a variety of use cases.
	  ◦ Sign your application code so you can ensure that your software remains secure, unaltered, and authentic.
	Create digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments.

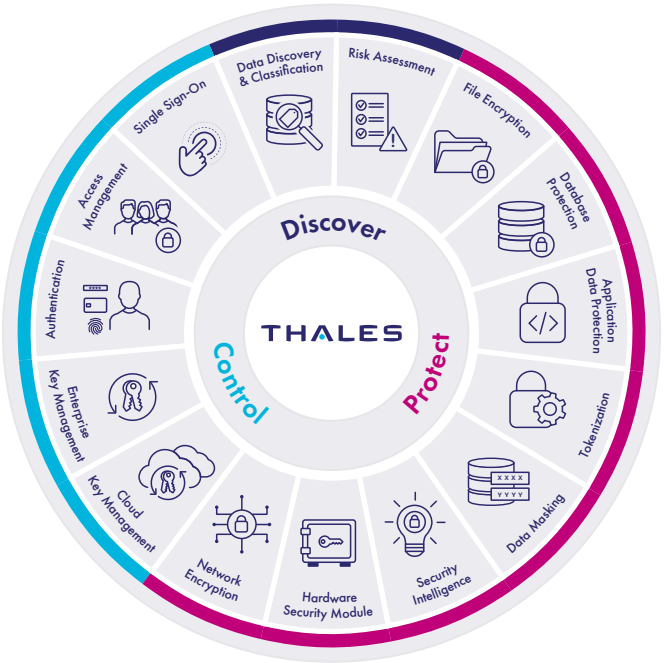
Key Takeaways

- Simplify data security, and accelerate time to compliance
- Secure sensitive data at rest with encryption/ tokenization
- Centralize cryptographic key management for hybrid and multi-cloud environments
- Offers granular access control

STDB Principle	Requirement Focus	Thales Solution
#1. STDB Governance Model	Segregation of duties, access control, audit log and reporting	CipherTrust Manager
#2. Identification of Critical Data	Evaluate critical data regularly	CipherTrust Data Discovery and Classification
#4. Critical Data Lifecycle Management	Encryption in-transit and at rest, prevent and detect unauthorized access	CipherTrust Transparent Encryption (CTE) Thales High Speed Encryptors (HSEs)
#5. Data Extraction and Ingestion	Protect cryptographic keys, encryption should be applied	CipherTrust Manager CipherTrust KMIP CipherTrust Transparent Database Encryption (TDE) Luna HSMs

Thales Data Protection Portfolio

With extensive experience in helping organizations comply with compliance requirements, Thales Cloud Protection & Licensing (CPL) can help organizations comply and recommend specific solutions through the "Discover, Protect and Control" strategy.



About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us