Compliance Brief

Data Security Compliance with the Guideline on ICT Security in Bangladesh

cpl.thalesgroup.com

THALES
Building a future we can all trust

Bangladesh Bank introduced the latest Guideline on ICT Security – version 4.0 that outlines how Banks and Financial Organizations (FOs) should manage IT and security risks and provide the Bank/FO with a better understanding of supervisory expectations regarding managing IT and security-related risks. Guideline on ICT Security – version 1.0 was first launched in Oct 2005, Version 4.0 is the latest and released in April 2023.

Digital transformation offers significant benefits to the financial ecosystem, but it also increases exposure to various technological risks, including cyber risks. The increasing complexity of information and communication technology (ICT) and consequent security risks have significant adverse impacts on the operations of financial organizations that might negatively affect the customers' interest, the organization's reputation and the nation's economy.

Information security is essential to protect organizational assets against these potential threats. Therefore, appropriate controls are required for an information security program with a broad and multi-layered security strategy.

Who needs to comply?

Guideline on ICT Security applies to Bank, Non-bank Financial Institute (NBFI), Mobile Financial Service Providers (MFSP), Payment Service Providers (PSP), Payment System Operator (PSO), White Label ATMs and Merchant Acquirers (WLAMA) and other financial service providers regulated by Bangladesh Bank.

Objective:

This Revised ICT Guideline defines minimum control requirements to which each Organization must adhere. The primary objectives of the Guideline are to:

1. Establish ICT Governance in the Financial Sector
2. Help Organizations develop their own ICT Security Policy
3. Establish standard ICT Security Management approach
4. Help Organizations develop secure and reliable ICT infrastructure
5. Establish a secure environment for the processing of data
6. Establish a holistic approach to ICT Risk management
7. Establish a procedure for Business Impact Analysis in conjunction with ICT Risk Management
8. Develop awareness of stakeholders' roles and responsibilities for the protection of information
9. Prioritize information and ICT systems and associated risks that need to be mitigated
10. Establish appropriate project management approach for ICT projects
11. Ensure best practices (industry standard) of the usage of technology
12. Develop a framework for timely and effective handling of operation and information security incidents
13. Mitigate any interruption to business activities and protect critical business processes from the effects of significant failures of information systems or disasters and ensure timely resumptions
14. Define necessary controls required to protect data transmitted over communication networks
15. Ensure that security is integrated throughout the lifecycle of information system acquisitions, development and maintenance
16. Minimize security risks for electronic banking infrastructure, including ATM and POS devices, payment cards, internet banking, mobile financial services, etc.
17. Build awareness and train the users associated with ICT activities for achieving the business objectives
18. Harbor safe and secure usage of emerging technologies.

How can Thales help with the Guideline on ICT Security?

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

Thales enables Banks and Financial Organizations in Bangladesh to align with the following six chapters in the **Guideline on ICT Security**.

Guidelines	Thales Solutions
Chapter 4: ICT Service Delivery Management	
4.5.3.1: The Organization shall ensure that appropriate **cryptographic key management** is in place, as well as validate the CSP's ability to **restore the service** from backups effectively. **4.5.3.2:** The Organization shall ensure that the cloud service provider (CSP) has formalized and tested processes and systems in place to **securely generate and manage cryptographic keys** in line with the Organization's requirements. **4.5.3.3:** The **data at rest** on the cloud and in **transit s**hall be **encrypted** as per the Organization's requirement. **4.5.3.4:** CSP shall ensure a standard **encryption algorithm** for data at rest and data in transit. **4.5.3.5: Sensitive data** including data backups shall be subject to **appropriate encryption** controls both in transit and at-rest. **4.5.3.6: Encryption keys** used for the encryption of the Organization's data shall be unique and not shared with others.	CipherTrust Cloud Key Management allows organizations to separate the keys from the data stored in the cloud, preventing unauthorized data access by the Cloud Service Provider by using the Hold-Your-Own-Key (HYOK) technology, organizations retain full control and ownership of their data by controlling encryption key access. **Protect Data at Rest:** CipherTrust Data Security Platform provides multiple capabilities for protecting data at rest in files, volumes, and databases. Among them: • CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management and privileged user access control. This protects data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. • CipherTrust Tokenization permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data, without exposing sensitive data during the analysis or in reports. **Protect Data in Motion:** Thales High Speed Network Encryption (HSE) provide network-independent, data-in- motion 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.
Chapter 5. Infrastructure Security Management	
5.3.1 – Data Classification **5.3.1.1:** The Organization shall have a well-defined process for data classification where it mentions how it classifies and labels data **5.3.1.4:** The Organization shall be aware of Personal Identifiable Information (PII), not to expose it to unintended parties. PII shall only be used if required and with confidentiality.	CipherTrust Data Discovery and Classification enables organizations to efficiently locate and classify structured and unstructured regulated data across multiple data sources as per major global and regional compliance requirements. Built-in templates offer rapid identification of regulated data, highlight security risks, and help uncover compliance gaps.
5.6.1 – WAN Management **5.6.1.2:** A mechanism shall be in place to encrypt and decrypt sensitive data traveling through WAN or public networks.	Thales High Speed Network Encryption (HSE) solutions provide network-independent data-in-transit/ motion 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.
5.9 – Database Security Management **5.9.3:** All types of access to any database containing cardholder or confidential data (including access by applications, administrators, and all other users) shall be restricted. **5.9.10:** Cryptographic Services shall be used to protect and validate critical information at rest and in transit	CipherTrust Transparent Encryption delivers database agnostic data-at-rest encryption with centralized key management, privileged user access control, and detailed data access audit logging that helps organizations meet compliance and best practice requirements for protecting data.

Guidelines	Thales Solutions
5.18 – Cryptography The most critical aspect of data encryption is the **protection and secrecy of cryptographic keys**, whether master keys, key encrypting keys or data encrypting keys. **5.18.2:** The Organization shall ensure encryption in 'data at rest' and 'data in transit' for critical data. **5.18.12:** The Organization should establish cryptographic key management policy and procedures covering generation, distribution, installation, renewal, revocation, and expiry **5.18.18:** The Organization shall maintain a backup of cryptographic keys. The same level of protection as the original cryptographic keys shall be accorded to backup keys.	**Thales Luna Hardware Security Modules (HSM)** and **Thales Key Management** should be used for key generation, storage and end-to-end key lifecycle management that is FIPS 140-2 compliant. **Hardware Security Modules (HSMs)** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Luna HSMs are available on-premises, in the cloud as-a-service, across hybrid environments and allow taking backup of keys in FIPS 140-2 level 3 compliant Backup HSMs. **Thales Key Management** offerings streamline and strengthen key management in cloud and enterprise environments over a diverse set of use cases. Leveraging FIPS 140-2-compliant virtual or hardware appliances, Thales key management tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications. It simplifies key lifecycle management including activities such as key generation, backup and restore, deactivation and deletion.
Chapter 9: Business Continuity Management	
9.2.2 Data Backup and Restore Management **9.2.2.7:** The Organization shall encrypt backup data in tapes or disks containing sensitive or confidential information before being transported offsite for storage.	Sensitive information in tapes or disks can be secured with **CipherTrust Data Security Platform** which ensures the data is encrypted before being stored and transported. **Thales Key Management** integrates with the leading backup solution vendors to manage the backup encryption keys and to separate the data from the keys. It also secures the data before it is backed up and stored in the removable media.
Chapter 10: Acquisition and Development of Information Systems	
10.8 – Application Programming Interfaces (APIs) Management **10.8.3:** The standards should include measures to protect the API keys or access tokens, which authorize access to APIs to exchange confidential data. A reasonable timeframe for access token expiry should be defined and enforced to reduce the risk of unauthorized access. **10.8.5:** Strong encryption standards and key management controls should be adopted to secure the transmission of sensitive data through APIs.	**CipherTrust Secrets Management (CSM)** is a state-of-the-art Secrets Management solution, powered by the Akeyless, which protects and automates access to mission-critical secrets across DevOps tools and cloud workloads, including secrets, credentials, certificates, API keys, and tokens. **CipherTrust Data Protection Gateway** offers transparent data protection to any RESTful web service or microservice leveraging REST APIs.
Chapter 11: Digital Payment Security	
11.2: POS Standards 11.2.5 The Organization shall implement Point-to-Point Data Encryption for all POS terminals **11.5: Payment Cards** 11.5.1 The Organization shall further ensure that sensitive card data is encrypted to ensure the confidentiality and integrity of these data in storage and transmission.	**payShield 10k HSM** is a payment hardware security module (HSM) used extensively throughout the global payment ecosystem by issuers, service providers, acquirers, processors and payment networks. It plays a fundamental security role in securing the payment credential issuing, user authentication, card authentication and sensitive data protection processes for both face-to-face and digital remote payments.

Guidelines	Thales Solutions
Chapter 14: Emerging Technology Management	
14.5 – Distributed Ledger Technology **14.5.5:** The Organization shall establish and agree on the architecture and procedure for implementing the Hardware Security Module (HSM) for securing Block Chain identity keys	**Thales Luna Network HSMs** are designed to store the private keys used by blockchain members to sign all transactions in a FIPS 140-2 Level 3 dedicated cryptographic processor. Keys are stored throughout their lifecycle; ensuring cryptographic keys cannot be accessed, modified or used by unauthorized devices or people.

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