



A Compilation of Regulatory Mandates in Singapore

Public Sector Data Security For
Government Agencies

The Notice On Cyber Hygiene
For Financial Industry (FI)

Cybersecurity Act For Critical
Information Infrastructure (CII)
& Others

Contents

03	Introduction
03	The need for compliance and regulatory standards
04	Thales tools for compliance to data security regulations and standards
07	Types of regulations mandated by the Government of Singapore
07	Public Sector Data Security (Government)
21	The Notice on Cyber Hygiene for Financial Industry (FI)
21	What is the regulation?
21	Whom will it impact?
21	Why is there a need for the regulation?
22	When was it implemented?
22	How can Thales Help?
24	Cybersecurity Act for Critical Information Infrastructure (CII) & Others
24	What is the regulation?
24	Whom will it impact?
24	Why is there a need for the regulation?
25	When was it implemented?
25	How can Thales help?
26	About Thales Cloud Protection & Licensing
27	References

Introduction

■ The need for compliance and regulatory standards

Today, it is imperative for professionals working in Singapore, and with its people and businesses, to understand the importance to enterprises of compliance with this country's digital security standards and regulations as well as the repercussions of failing to comply. This document reviews recent laws and standards put forth by Singaporean authorities and provides strategies for complying with them.

But what is compliance? How do businesses achieve it? And how do they remain compliant?

For our discussion, compliance means organisations and their employees abide by the mandatory laws, regulatory standards, and ethical practices put forth by authorities in Singapore, such as the Government of Singapore, and the Monetary Authority of Singapore (MAS), to ensure digital security.

The Singapore government and MAS have made great strides in achieving digital security across the country by enacting laws and regulations for this purpose. Compliance with those laws and regulations will ensure that Singapore continues to be a digitally safe place to do business for both customers and the businesses themselves.



■ Thales tools for compliance to data security regulations and standards

In our review below of the data security regulations of Singapore, we note where and how Thales Cloud Protection & Licensing (CPL) can help organisations comply and with which specific products. In this section, we quickly review those products and provide links to more information on each.

Data security measures called for in virtually all regulations and standards

Thales CPL is a leader in digital security, and, having helped hundreds of enterprises comply with regulatory regimes around the world, we recommend key data protection technologies called for in virtually every set of regulations. These include:

- Data access control
- Encryption and tokenisation (pseudonymisation) of data at rest
- Encryption of data in motion
- Encryption key management
- Keeping and monitoring user access logs
- The use of hardware security modules for protecting encryption keys and executing encryption processes

Data access control

Thales CPL's **CipherTrust Manager (CM)** enables the organisation to limit user access privileges to information systems that contain sensitive Information and orchestrates the CipherTrust Data Security Platform, which makes it easy to manage data at rest security across your organisation.

SafeNet Trusted Access (STA) is a cloud-based access management service that combines the convenience of cloud and web single sign-on (SSO) with granular access security. By validating identities, enforcing access policies and applying Smart Single Sign-On, organisations can ensure secure, convenient access to numerous cloud applications from one easy-to-navigate console.

Adding Thales's SafeNet certificate-based authentication (CBA) smart card solution as an integral part of IT infrastructure significantly improves client logon security by requiring multi-factor authentication. Adding multiple factors ensures secure login to workstations and enterprise networks, eliminates complex and costly passwords, and significantly reduces help desk calls.

With **SafeNet Authentication and Access Management solutions** you can leverage a unified authentication infrastructure for both on-premises and cloud-based services—providing a centralized, comprehensive way to manage all access policies. Users can log into enterprise cloud services such as Office 365, Salesforce.com or GoogleApps through their existing SafeNet authentication mechanisms.

Encryption and tokenisation

Thales CPL's **CipherTrust Transparent Encryption Suite (CTE)** protects data with file and volume level data-at-rest encryption, access controls, and data access audit logging without re-engineering applications, databases, or infrastructure. Deployment of the transparent file encryption software is simple, scalable and

fast, with agents installed above the file system on servers or virtual machines to enforce data security and compliance policies. Policy and encryption key management are provided by the CipherTrust Data Security Manager.

CipherTrust Tokenization dramatically reduces the cost and effort required to comply with security policies and regulatory mandates. The solution delivers capabilities for database tokenisation and dynamic display security. Enterprises can efficiently address their objectives for securing and pseudonymising sensitive assets—whether they reside in data centre, big data, container, or cloud environments.

CipherTrust Application Encryption (CAE) delivers key management, signing, and encryption services enabling comprehensive protection of files, database fields, big data selections, or data in platform-as-a-service (PaaS) environments. The solution is FIPS 140-2 Level-1 certified, based on the PKCS#11 standard and fully documented with a range of practical, use-case based extensions to the standard. CipherTrust Application Encryption eliminates the time, complexity, and risk of developing and implementing an in-house encryption and key management solution. Development options include a comprehensive, traditional software development kit for a wide range of languages and operating systems as well as a collection of RESTful APIs for the broadest platform support.

The **CipherTrust Developer Suite** is a set of products that streamline development efforts to add encryption, tokenisation, masking, and other cryptographic functions to applications. The job of the developer is made easy and fast by leveraging sample code and APIs that are best for their environment, while key management functions are kept separate and secure in a FIPS 140-2 hardware or virtual appliance that is operated by IT or SecOps. Securing data

at the application, with separation of duties for key management, provides the highest levels of protection and compliance. The **CipherTrust Developer Suite** also includes applications and utilities that leverage the core components to add security layers to databases and other structured data stores.

Sensitive Data Discovery and Classification

Thales CipherTrust Data Discovery and Classification helps your organization get complete visibility into your sensitive data with efficient data discovery, classification, and risk analysis across heterogeneous data stores - the cloud, big data, and traditional environments - in your enterprise.

Encryption of data in motion

A powerful safeguard for data in motion, **Thales High-Speed Encryptors (HSE)** deliver high-assurance certified data in motion encryption capabilities that meet secure network performance demands for real-time low latency and near zero overhead to provide security without compromise for data on the move across the network.

Encryption key management

Thales CPL's **CipherTrust Enterprise Key Management** unifies and centralizes encryption key management on premises and provides secure key management for data storage solutions. Cloud Key Management products include the **CipherTrust Cloud Key Manager (CCKM)** for centralized multi-cloud key life cycle visibility and management with FIPS-140-2 secure key storage, and Cloud Bring Your Own Key.

User access logs

CipherTrust Security Intelligence Logs let your organisation identify unauthorized access attempts and build baselines of authorized user access patterns. CipherTrust Security Intelligence integrates with leading security information and event management (SIEM) systems that make this information actionable. The solution allows immediate automated escalation and response to unauthorized access attempts. It also provides all the data needed to specify behavioral patterns required to identify suspicious use by authorized users, as well as for training.

Hardware security modules

Thales Hardware Security Modules (HSM) provide the highest level of encryption security by always storing cryptographic keys in hardware. Thales HSMs provide a secure crypto foundation, because the keys never leave the intrusion-resistant, tamper-evident, FIPS-validated appliance. Strong access controls prevent unauthorized users from accessing sensitive cryptographic material, since all cryptographic operations occur within the HSM. In addition, Thales CPL implements operations that make the deployment of secure HSMs as easy as possible, and our HSMs are integrated with Thales Crypto Command Center for quick and easy crypto resource partitioning, reporting and monitoring.

The award winning **Thales Data Protection On Demand (DPoD)** solution is a cloud-based platform providing a wide range of cloud HSM and key management services through a simple online marketplace. These include HSM on Demand and Key Management on Demand.



Types of regulations mandated by the Government of Singapore

■ Public Sector Data Security (Government)

What is the regulation?

The Singapore Government is reaffirming the importance of data security while “seeking the views of industry and global experts to recommend a slate of technical measures to strengthen data safeguards.”ⁱ

The announcement was made by the Public Sector Data Security Review Committee, which was convened by Prime Minister Lee Hsien Loong in March 2019.

The Committee has completed its work November 2019 and the Public Sector Data Security Review Committee (PSDSRC) report contains five key recommendations for the public sector, which when implemented would:

- (a) Effectively protect against data security threats and minimise the occurrence of data incidents;
- (b) Detect and respond to data incidents in a swift and decisive manner, and learn from each incident;
- (c) Build data security competencies and inculcate a culture of excellence around sharing and using data securely;

(c) Build data security competencies and inculcate a culture of excellence around sharing and using data securely;

(d) Raise the accountability and transparency of the public sector data security regime; and

(e) Put in place the organisational structures to sustain a high level of security, and to be adaptable to new challenges.

The Committee’s recommendations will address existing gaps and build a data security regime that is resilient as technology advances, systems become more integrated, and risks become increasingly multi-faceted.

Key Recommendations

These recommendations cover Government and non-Government Entities that handle public sector data to deliver public services, perform operational processes, or provide consultation services for policy planning.

Desired Outcome	Key Recommendations
Protects data and prevents data compromises	1. Enhance technology and processes to effectively protect data against security threats and prevent data compromises.
Detects and responds to data incidents	2. Strengthen processes to detect and respond to data incidents swiftly and effectively.
Competent public officers embodying a culture of excellence	3. Improve culture of excellence around sharing and using data securely, and raise public officers' competencies in safeguarding data
Accountability for data protection at every level	4. Enhance frameworks and processes to improve the accountability and transparency
Sustainable and resilient manner	5. Introduce and strengthen organisational and governance structures to drive a resilient public sector data security regime that can meet future needs.

* Information from Public Sector Data Security Review Committee (PSDSRC)

Whom will it impact?

The in-depth investigations of the IT systems will revolve around five agencies that deal with high volumes of sensitive data:

- Ministry of Health
- Health Sciences Authority (HSA)
- Health Promotion Board (HPB)
- Central Provident Fund Board
- Inland Revenue Authority of Singapore

Why is there a need for the regulation?

The strong fundamentals of Singapore's current security regime need to be reinforced, because there are increasing demands for valuable data to make better policies and offer digital services to the public at the very time that the IT landscape is becoming progressively more complex.

The regulation will enable government organisations to secure and protect citizens' data end to end and will include vendors and other authorized third parties. This is expected to encourage public confidence and deliver improved public service to the people of Singapore.

All public sector agencies will be able to maintain the highest standards of data governance, bolstering the efforts taken for the vision of the Smart Nation.

When will it be implemented?

The Government targets to implement the measures in 80 per cent of Government systems by end-2021. The timeline for remaining 20 per cent which involve systems which are complex or require significant redesign is end-2023. In the interim, agencies will put in place appropriate measures to manage the relevant data risks.



For this handbook, Thales Cloud Protection & Licensing (CPL) will list out available solutions to address PSDSRC's Key Recommendation 1, specifically on the **technical measures (prefixed with 'T')**.

Key Recommendation 1: Enhance technology and processes to effectively protect data against security threats and prevent data compromises.

The Committee has proposed 13 technical (prefixed with 'T') and 10 process safeguards (prefixed with 'P'). These will be incorporated into ICT and data systems in different combinations depending on the data security risks that the system is expected to face. They will minimise the risk of data compromises by achieving the following:

Recommendation 1.1: Reduce the surface area of attack by minimising data collection, data retention, data access and data downloads.



Collect and retain data only when necessary

P1: Collect datasets only where necessary

P2: Limit retention period of data



Minimise the proliferation of data to endpoint devices

P3: Isolated Secured Environments for third parties and privileged users

P4: Access data by queries instead of data dumps

P5: Access sensitive files on secured platforms



Access and use data for the task at hand

T1: Volume limited and time limited data access

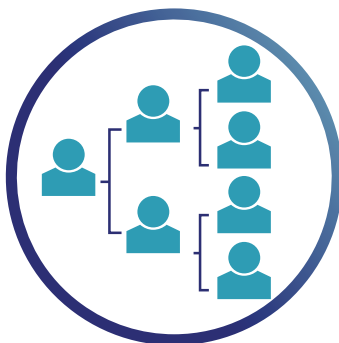
T2: Automatic Identity and Access Management Tools

P6: Limit and monitor authorised and privileged access

T2. Automatic identity and access management (IAM) tools

Description	Ensures that access to the data is limited to only authorized people. IAM tools automatically manage officers' identity and access rights, ensuring that only authorized persons can access data. In addition to IAM, automatic privileged identity and management (PIM) tools control, monitor, and protect user accounts, which have more access and capabilities than ordinary users (e.g. administrator accounts). More stringent measures (e.g. 2-Form Factor Authentication, time-limited access) are required to protect these accounts.
Issues addressed	Confidentiality at usage phase
Illustrative example	Suppose an officer previously took on a role in Ministry of Health that authorized him to look at the infectious disease database. When that officer relinquishes that role by moving to another department, the IAM will ensure that he will no longer have any access to the infectious disease dataset.
Thales proposal	STA-Basic / STA
	SafeNet Trusted Access is an access management service that combines the convenience of single sign-on with context-sensitive access security. Contextual authentication creates compliance-based access policies to prevent security fatigue. It validates identity by taking into account variables, such as your network, location and operating system. Contextual data provides additional information on a login attempt, and initiates the appropriate access policy.

Recommendation 1.2: Enhance the logging and monitoring of data transactions to detect high-risk or suspicious activity.



Enhance logs and records to more accurately pinpoint high-risk activity and assist in response and remediation

P7: Maintain data lineage

T3: Digital watermarking of files



Detect suspicious activity and alert the user or stop the unauthorised activity automatically

T4: Enhanced logging and active monitoring of data access

T5: Email data protection tool

T6: Data loss protection tool

T4. Enhanced logging and active monitoring of data access

Description	Keeps logs and analyses them to flag anomalous activity as well as support remediation in the event of a data breach. Logs access to sensitive data in greater detail, such as at the individual data query level. The logs should be protected from accidental or deliberate erasure, so that they can reliably show what data has been compromised, how it has been compromised, and who was involved in the compromise. Active monitoring of the log files and network traffic help to detect anomalies and potential malicious activities.
Issues addressed	Confidentiality, integrity at usage phase
Illustrative example	Suppose a malicious actor performs an attack over a long period of time. The individual actions by the malicious actor at each point in time might not raise any red flags; however, his actions over time might be suspicious. By storing and analysing the detailed logs, these anomalous activities over time will be flagged.
Thales proposal	<p>CipherTrust Transparent Encryption Suite (CTE) + CipherTrust Security Intelligence</p> <p>CipherTrust Security Intelligence provides support for Security Information and Event Management (SIEM) products such as ArcSight, Splunk and QRadar. CipherTrust Security Intelligence, combined with a SIEM product, provides solutions that monitor real-time events and analyse long-term data to find anomalous usage patterns, qualify possible threats to reduce false positives, and alert organisations when needed.</p>

Recommendation 1.3: Protect the data directly when it is stored and distributed to render the data unusable even when extracted or intercepted.



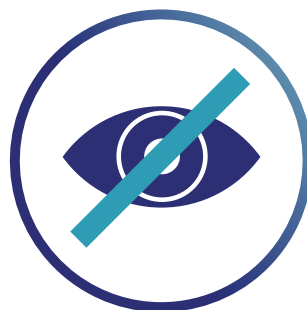
Render data unusable even if exfiltrated from storage

T7: Hashing with salt

T8: Tokenisation

T9: Field-level encryption

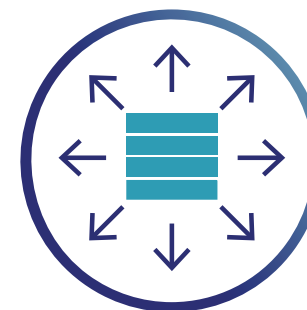
P8: Managing keys to these safeguards



Partially hide the full data

T10: Obfuscation / masking / removal of entity attributes

T11: Dataset partitioning



Protect the data during distribution

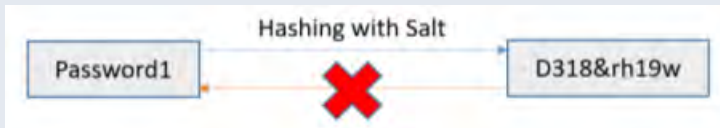
T12: Password protecting and encrypting data files.

P9: Securely distribute password out-of-band.

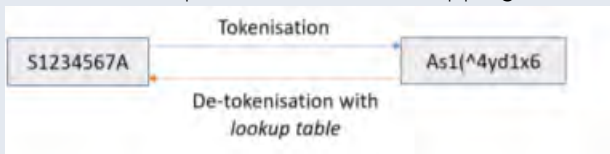
T13: Data file integrity verification

P10: Distribute files through appropriate secure channels.

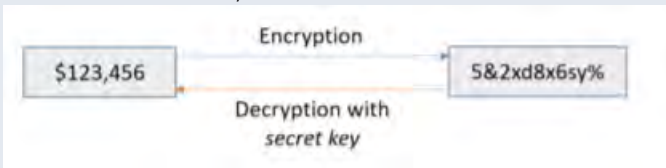
T7. Hashing with salt

Description	Ensures that sensitive values cannot be seen or reasonably recovered in the event of a compromise. This measure is appropriate for data fields where the actual values need not be recovered, such as passwords. This technique will replace sensitive values with algorithmically derived values that cannot be reversed easily.
Issues addressed	Confidentiality at storage phase
Illustrative example	<p>Illustrative Example: Suppose a malicious actor manages to extract a database which stores user accounts and passwords. If “hashing with salt” has been applied to the original passwords, the malicious actor would not be able to see or recover them.</p> 
Thales proposal	<p>CipherTrust Manager (CM) + CipherTrust Developer Suite</p> <p>CipherTrust Developer Suite is an application encryption library providing a standards-based API to do cryptographic operations like hashing, encryption, signing, etc., using keys from the CipherTrust Manager (CM).</p>

T8. Tokenisation


Description	Ensures that identifiers cannot be seen in the event of a compromise. This measure replaces identifiers and attributes with a different value known only to the authorised users. This technique is appropriate for data fields where the actual values need to be recovered, such as identifiers required for service delivery.
Issues addressed	Confidentiality at storage phase
Illustrative example	<p>Suppose a malicious actor manages to extract a database which stores NRICs. Unless the malicious actor manages to obtain the token lookup table (i.e. the full mapping of values to tokens), the perpetrator would not be able to see the original NRIC.</p> 
Thales proposal	<p>CipherTrust Manager (CM) + CipherTrust Tokenization</p> <p>CipherTrust Tokenization is a vaulted/vault-less tokenisation service used for replacing sensitive data with tokenised data. Tokenised data retains the format of the original data while protecting it from theft or compromise.</p>

T9. Field-level encryption

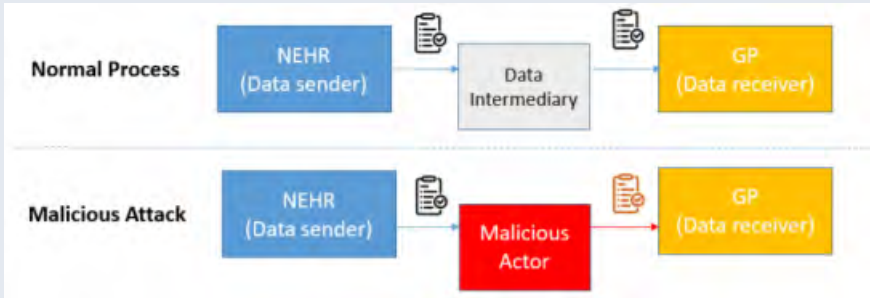
Description	Ensures that sensitive values cannot be seen in the event of a compromise. It involves encrypting specific data fields to hide the true value. A different secret encryption key is used for each field. The underlying technique of field-level encryption achieves the same function as Tokenisation, but is applied to different elements in the database (i.e. identifiers vs attributes). The technical implementation of field-level encryption uses a mathematical encryption function instead of the lookup table used for tokenisation.
Issues addressed	Confidentiality at storage phase
Illustrative example	<p>Suppose a malicious actor manages to extract a database which stores income. Unless the malicious actor manages to obtain the secret key, he or she would not be able to see the original value (income).</p> 
Thales proposal	<p>CipherTrust Manager (CM) + CipherTrust Application Encryption*</p> <p>CipherTrust Application Encryption* provides a framework to deliver application-layer encryption such as column- or field-level encryption in databases.</p>

*CipherTrust Application Encryption - Product name subject to change.

T10. Obfuscation/masking/removal of entity attributes

Description	Ensures that the exact sensitive values cannot be seen or ever recovered in the event of a compromise, although approximate or noisy values might still be seen. This involves hiding the true value of the attributes by adding noise, banding the data, or masking out portions of the value. Attributes not relevant for data usage should be removed. This measure is appropriate where the exact values are sensitive, but noisy values (that are less sensitive) are sufficient for usage and exploitation.
Issues addressed	Confidentiality at storage phase
Illustrative example	<p>Suppose an agency wishes to send customer service agents some NRIC for verification purposes. They might mask the first 5 characters before sending it over, as the last 4 characters are sufficient for verification.</p> 
Thales proposal	<p>CipherTrust Manager (CM) + CipherTrust Tokenization</p> <p>CipherTrust Tokenization provides Data masking capabilities that can be applied to any detokenised data to hide sections of the data from different groups of users. For example, less-privileged database users might view only the last four digits of a detokenised NRIC number, while a more privileged user could view the NRIC number.</p>

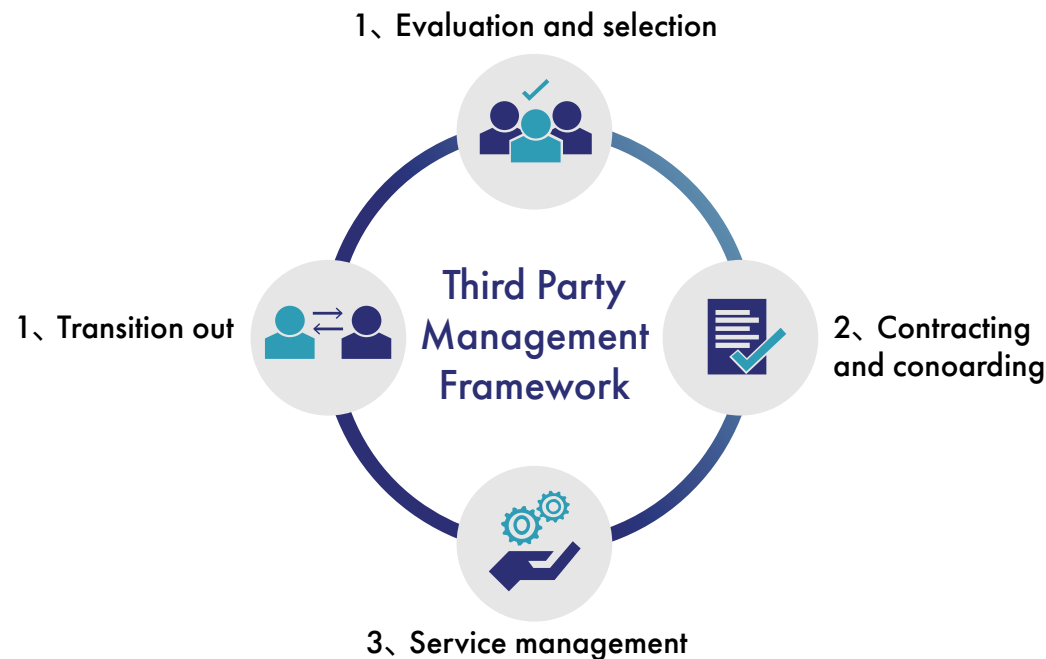
T13. Data file integrity verification

Description	Ensures that the receiver gets the same file that the original sender intended. This is done by the original data sender providing a checksum or digital signature that confirms the integrity of a data file.
Issues addressed	Integrity at distribution phase
Illustrative example	<p>Suppose the blood group data file of a group of patients is extracted from the National Electronic Health Record (NEHR) system and sent to their doctors through a hospital. A hospital staff person with malicious intent might modify a person's blood group and send the modified file to doctors. This will cause the patient harm as doctors will use the wrong blood group information for treatment, even though the underlying NEHR database has not been modified.</p>  <p>This measure allows the doctors to verify that the data file from the NEHR has not been changed along the way and protects against these attacks.</p>
Thales proposal	<p>CipherTrust Manager (CM) + CipherTrust Developer Suite</p> <p>CipherTrust Developer Suite supports hashing of data. To validate the integrity, hash of the data can be compared at the sender and receiver end.</p>

Recommendation 1.4: Develop and maintain expertise in advanced technical measures⁴.

Recommendation 1.5: Enhance the data security audit framework to detect gaps in practices and policies before they result in data incidents.

Recommendation 1.6: Enhance the third party management framework to ensure that third parties handle Government data with the appropriate protection.



The Committee has also identified six advanced technical measures, which are not sufficiently mature or readily integrate for widespread implementation:

(i) Homomorphic Encryption; (ii) Multi-party authorisation; (iii) Differential Privacy; (iv) Dynamic Data Obfuscation and Masking; (v) Digital Signing of Data File; and (vi) Secured File Format.

The Notice on Cyber Hygiene for Financial Industry (FI)

■ What is the regulation?

Recently, the Monetary Authority of Singapore (MAS) issued guidelines—Notice on Cyber Hygiene—to renew the cybersecurity standards and enhance cyber resilience across the finance industry. The authority has asked financial institutions to take measures to alleviate the rising risk of cyber threats.

The Notice will make the following requirements mandatory for financial institutions:ⁱⁱ

- Establish and implement robust security for IT systems
- Ensure updates are applied to address system security flaws in a timely manner
- Deploy security devices to restrict unauthorised network traffic
- Implement measures to mitigate the risk of malware infection
- Secure the use of system accounts with special privileges to prevent unauthorised access
- Strengthen user authentication for critical systems as well as systems used to access customer information

■ Whom will it impact?

The changes in the MAS Technology Risk Management (TRM) guidelines will impact organisations in the financial sector.

Financial companies will need to develop and implement robust security for IT systems, ensure timely updates to report system security flaws, and deploy security devices to regulate unauthorised network traffic. Additionally, financial institutions need to take steps to eliminate the risk of malware, secure system accounts to avert unauthorised access, and strengthen user authentication for critical systems as well as systems used to access customer information.

■ Why is there a need for the regulation?

The ongoing increase in financial sector cyber threats prompted this regulation.

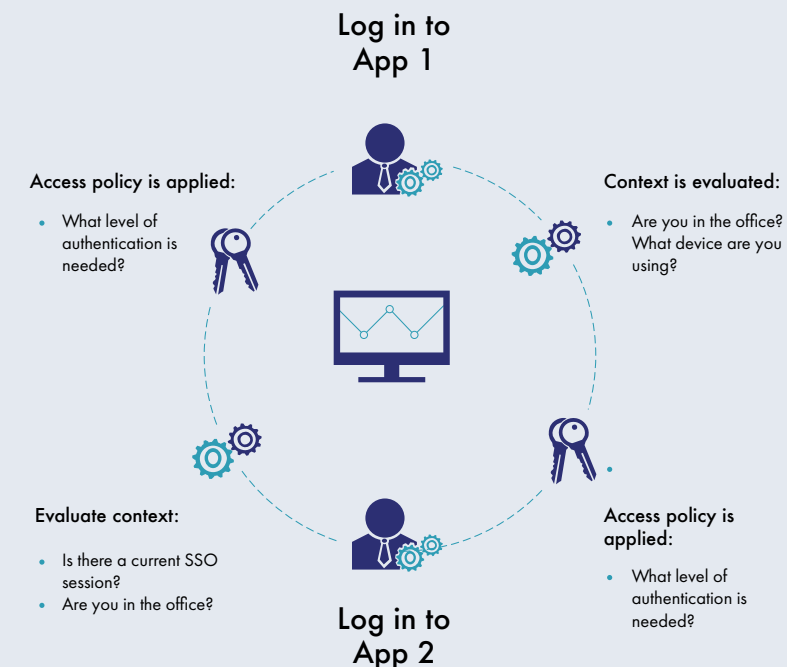
In September 2018, MAS sought feedback from the citizens of Singapore on the proposal to make the suite of cybersecurity practices into legal guidelines. The finance industry appreciated the measures taken by MAS and put forward suggestions about the execution of the guidelines, which included focusing on strengthening user access to systems that store or access customer data, and allowing more time for financial organisations to design, acquire and integrate robust user authentication technology into their key systems.

■ When was it implemented?

The notice went into effect August 6, 2020.ⁱⁱⁱ

■ How can Thales Help?

Mandate	Thales Proposal
Establish and implement robust security for IT systems;	<p>Thales recommends three different approaches.</p> <ol style="list-style-type: none"> 1. Bring Your Own Key (BYOK), when the application or IT system can provide crypto capability, keys can be stored and managed using CipherTrust's key manager. 2. Bring Your Own Encryption (BYOE), when the application or IT system does not provide crypto capability, use CipherTrust's transparent encryption agent to encrypt data in the database or files system. 3. CipherTrust Application Crypto Suite (VACS), for IT systems that require the highest security. Protect data using CipherTrust's application crypto suite to protect data in the application layer. Data should be encrypted by the application using VACS before going into the databases or file system.
Ensure updates are applied to address system security flaws in a timely manner;	N/A
Deploy security devices to restrict unauthorised network traffic;	N/A
Implement measures to mitigate the risk of malware infection;	N/A
Secure the use of system accounts with special privileges to prevent unauthorised access.	Thales SafeNet Trusted Access provides step up authentication for system account to prevent unauthorized access and/or integrate with different PAM/PIM solutions to provide step up authentication for privileged accounts.

Mandate	Thales Proposal
<p>Strengthen user authentication for critical systems as well as systems used to access customer information.</p>	<p>Use SafeNet Trusted Access to provide both MFA and contextual base authentication for system accounts. Contextual authentication is central to creating compliance-based access policies and preventing security fatigue. Taking into account variables, such as your network, location and operating system, contextual data provides additional information on login attempts, and initiates the appropriate access policy. By assessing a user's contextual login attributes, single sign on and access management solutions can continuously match the level of authentication required from the user with the access policy defined for each application. In this manner, authentication is applied granularly—in the most frictionless manner possible—per an application's access policy, rather than as a blanket, uniform rule for all enterprise resources.</p>  <p>Log in to App 1</p> <p>Access policy is applied:</p> <ul style="list-style-type: none"> What level of authentication is needed? <p>Context is evaluated:</p> <ul style="list-style-type: none"> Are you in the office? What device are you using? <p>Evaluate context:</p> <ul style="list-style-type: none"> Is there a current SSO session? Are you in the office? <p>Log in to App 2</p> <p>Access policy is applied:</p> <ul style="list-style-type: none"> What level of authentication is needed?

Cybersecurity Act for Critical Information Infrastructure (CII) & Others

What is the regulation?

The Cybersecurity Act 2018 is a new law that creates a regulatory framework for monitoring and reporting cybersecurity threats to essential services in the country.^{iv}

Its four key objectives are to:

- Strengthen the protection of Critical Information Infrastructure (CII) against cyber-attacks
- Authorise CSA to prevent and respond to cybersecurity threats and incidents
- Establish a framework for sharing cybersecurity information
- Establish a light-touch licensing framework for cybersecurity service providers

Whom will it impact?

The Act provides for the appointment of a Cybersecurity Commissioner as a regulator for the sector. The Act confers on the Commissioner significant powers to respond to and prevent cybersecurity incidents affecting Singapore. These powers apply to all computer or computer systems in Singapore and are not limited to Critical Information Infrastructure (CII).

A key thrust of the Act is the imposition of cybersecurity obligations on public and private cyber owners of CII that are used to provide essential services.

The 11 critical sectors of essential services that are identified in the Act are energy, info-communications, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, government, and media.

Why is there a need for the regulation?

Ongoing cybersecurity incidents highlight the need for a coordinated public response, which the Act address from the Singapore perspective. However, given the borderless nature of cyberspace, a coordinated international response will be required.

From a business perspective, the largest impact arising from this Act is likely to be the designation of CII owners and the cybersecurity obligations imposed on them.

Additionally, the licensing of certain cybersecurity services may lead to customers being more selective as to the cybersecurity vendors they use. As the licensing regime will increase the compliance costs for licensed cybersecurity service providers, they may seek to increase their fees to recover this cost.

■ When was it implemented?

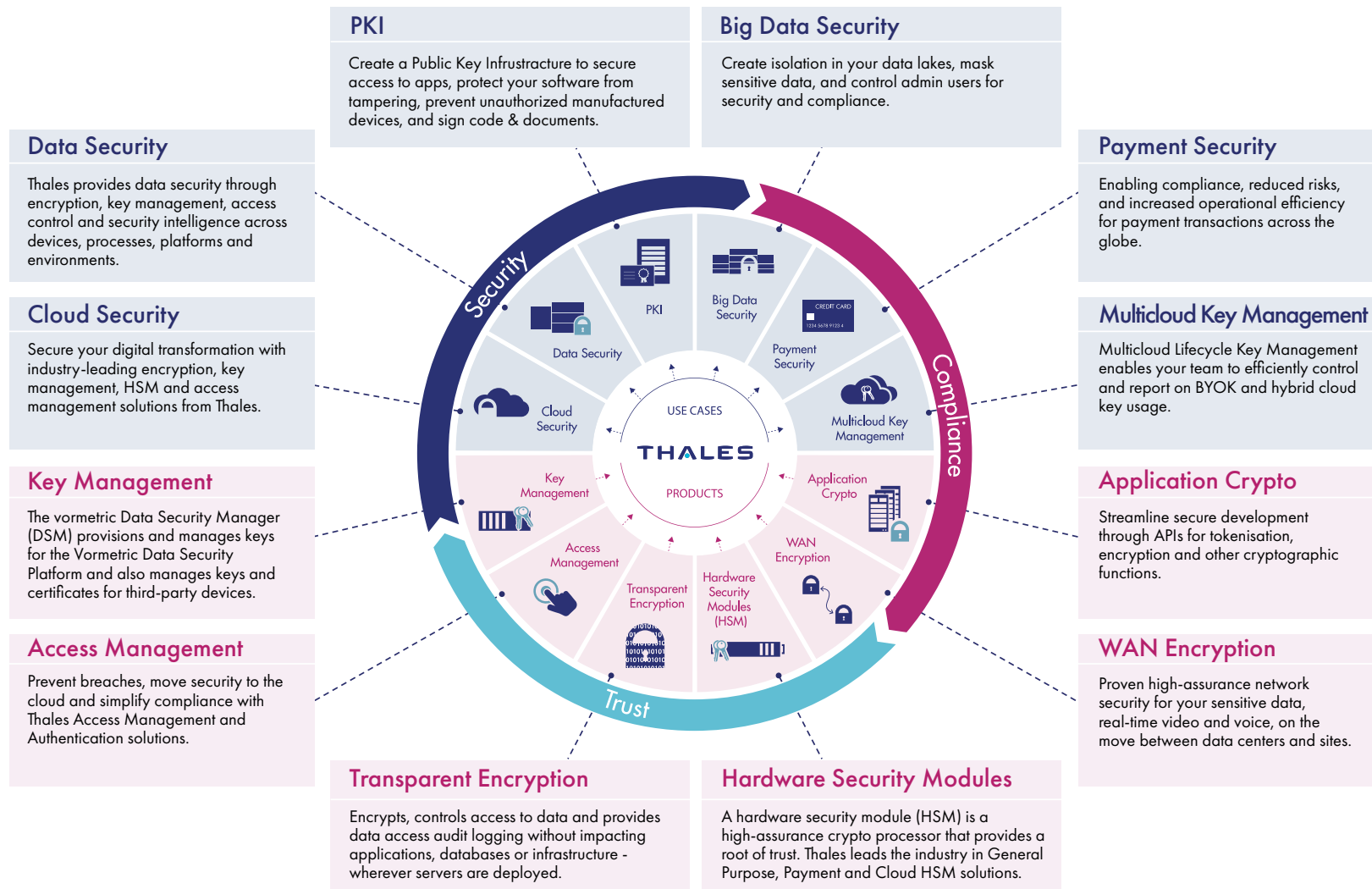
The Singapore Parliament passed the Cybersecurity Act 2018 (Act. 9 of 2018) on 5 February 2018. It came into effect 31 August 2018.

■ How can Thales help?

It is currently not clear what will be expected of organisations as a result of this Act. However, in “Thales tools for compliance to data security regulations and standards” in the introduction to this document, we outline the best practices we see called for in virtually all data security regulations. We also provide information on the tools we provide to aid organisations in their efforts to comply.



About Thales Cloud Protection & Licensing



Today's enterprises depend on the cloud, data and software to make decisive decisions. That's why the most respected brands and largest organisations in the world rely on Thales to help them protect and secure access to their most sensitive information and software, wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

References

- ⁱ <https://www.smartnation.sg/whats-new/press-releases/progress-update-on-public-sector-data-security-review>
- ⁱⁱ <https://www.mas.gov.sg/news/media-releases/2019/mas-issues-new-rules-to-strengthen-cyber-resilience-of-financial-industry>
- ⁱⁱⁱ <https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Responses-to-Feedback-Received-to-Draft-Notice-on-Cyber-Hygiene---6-August.pdf?la=en&hash=30855EC539C0764709810E10F2F1260E9D96EBCB>
- ^{iv} <https://www.dataprotectionreport.com/2018/09/singapores-new-cybersecurity-act-come-into-force-heres-what-you-need-to-know/>
- ^v https://www.smartnation.gov.sg/docs/default-source/press-release-materials/psdsrc-main-report.pdf?sfvrsn=554b5830_2

Americas – Thales

Arboretum Plaza II,
9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA

 +1 888 343 5773

 [Contact Us](#)

EMEA – Thales

350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF

 +44 (0)1844 201800

 [Contact Us](#)

APAC – Thales

Thales, Units 4101, 41/F. 248 Queen's
Road East
Wanchai Hong Kong, PRC

 + 852 2815 8633

 [Contact Us](#)

Or visit our **Website**

