cpl.thalesgroup.com

THALES
Building a future we can all trust

A Review of the Monetary Authority of Singapore (MAS) Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption

Introduction

An increasing number of financial institutions ("FIs") are using public cloud services for their operations, as the COVID-19 pandemic continues to accelerate the pace of digital transformation. On 1 June 2021, the Monetary Authority of Singapore (MAS) issued an advisory highlighting some key risks and control measures that FIs should consider before adopting public cloud services. The advisory does not set out legal obligations per se, but instead offers specific guidance on managing cloud-related risks. In doing so, the advisory aims to supplement other MAS documents, which include the more general notices (e.g., on technology risk management and cyber hygiene for particular sectors) that set out legal requirements for FIs.

While using public cloud services can bring benefits to institutions, the services may also bring specific risks that need to be managed differently than traditional on-site IT infrastructure risks. For example, the advisory notes that many public cloud security incidents, such as data leaks, were caused by poor management on the user's end (e.g., poor control of access to the service provider's cloud).

Managing these specific risks requires tailor-made solutions. Thales's industry-leading products enable enterprises to centrally manage and secure access to applications, and to protect and remain in control of their data in the cloud and on-premises. SafeNet Trusted Access, Thales's Identity and Access Management (IAM) service, combines the convenience of single sign-on with context-sensitive access security and multi-factor authentication (MFA)-- aligning with the same zero trust principles that are recommended in the MAS advisory. As for Data Protection, our suite of solutions, ranging from data discovery and classification and data encryption to key management, allows our clients to discover, protect and control sensitive data as the data is transferred to and while it remains in the cloud, working alongside the provider's security system.

About the Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption

What is it?

The Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption is a paper issued by the MAS in response to the increasing adoption of public cloud services by FIs.

The advisory aims to guide FIs in managing cloud-related threats and minimizing security incidents by laying out some of the more common key risks and corresponding control measures that FIs should consider before moving data and processes to the cloud. The control measures include:

- Developing a public cloud risk management strategy that takes into consideration the unique characteristics of public cloud services;
- Implementing strong controls in areas such as Identity and Access Management (IAM), cyber security, data protection and cryptographic key management;
- Expanding cyber security operations to include security of public cloud workloads;
- Managing cloud resilience, outsourcing, vendor lock-in and concentration risks; and
- Ensuring that staff have the skills to manage public cloud workloads and risks.

The advisory also touches on which aspects cloud service providers and FIs are responsible for, and which control measures might be shared between them, depending on their particular arrangement. In the end, however, the advisory notes that FIs are "ultimately responsible and accountable for maintaining effective oversight and governance of their engagement with [providers of cloud services]".

This specific guidance on cloud-related risks supplements other MAS documents, including more general notices (e.g., on technology risk management and on cyber hygiene for all aspects of IT) that set out legal requirements for FIs, depending on which sector they are in. It also complements the MAS's Technology Risk Management Guidelines; the 2021 edition sets out higher expectations in terms of security controls and risk governance than the 2013 edition.

Why is there a need for it?

The increasing adoption of new technology, and utilization of existing tools in new ways, has enabled many FIs to optimize their processes through automation and to improve or add to their products and services. But the process of digital transformation comes with both benefits and potential risks. As systems become bigger and more interlinked because of institutions' operational requirements, their attack surface also expands, making them more vulnerable to increasingly sophisticated attacks by malicious actors. Without adequate security measures, systems could be compromised, leading to fraudulent financial transactions, leaks of sensitive data, and the disruption of systems essential for operations.

In response to this, the MAS has already issued several documents laying out requirements and guidelines for technology and cyber security risks. These documents have a relatively broad scope in terms of the technology they cover, and requirements vary per sector. But with more and more FIs adopting public cloud services as part of their digital transformation efforts accelerated by the COVID-19 pandemic, the MAS decided to issue specific guidance on public cloud services in June 2021.

The advisory lays out the risks unique to public cloud services to guide FIs in developing their risk management strategy. It also notes some best practices for mitigating cloud-specific threats. If FIs fail to establish the appropriate security measures, as recommended in the advisory, the data that they place in the cloud could be at risk of being compromised by malicious actors; in turn, any resulting security incidents could affect the ability of FIs to maintain their operational continuity, and fulfillment of their legal obligations.

Whom will it impact?

The advisory affects FIs regulated by the MAS. These include, but are not limited to the following sectors and institutions:

Banking	Capital Markets	Insurance	Banking
Deposit-taking institutions, including full banks, wholesale banks, merchant banks and finance companies	Capital markets entities, including trustees, dealers, credit rating agencies and financial advisers	Insurance companies and insurance brokers, including licensed insurers, authorised reinsurers and registered insurance brokers	Payment service providers and payment systems, including clearing and settlement systems

When was it implemented?

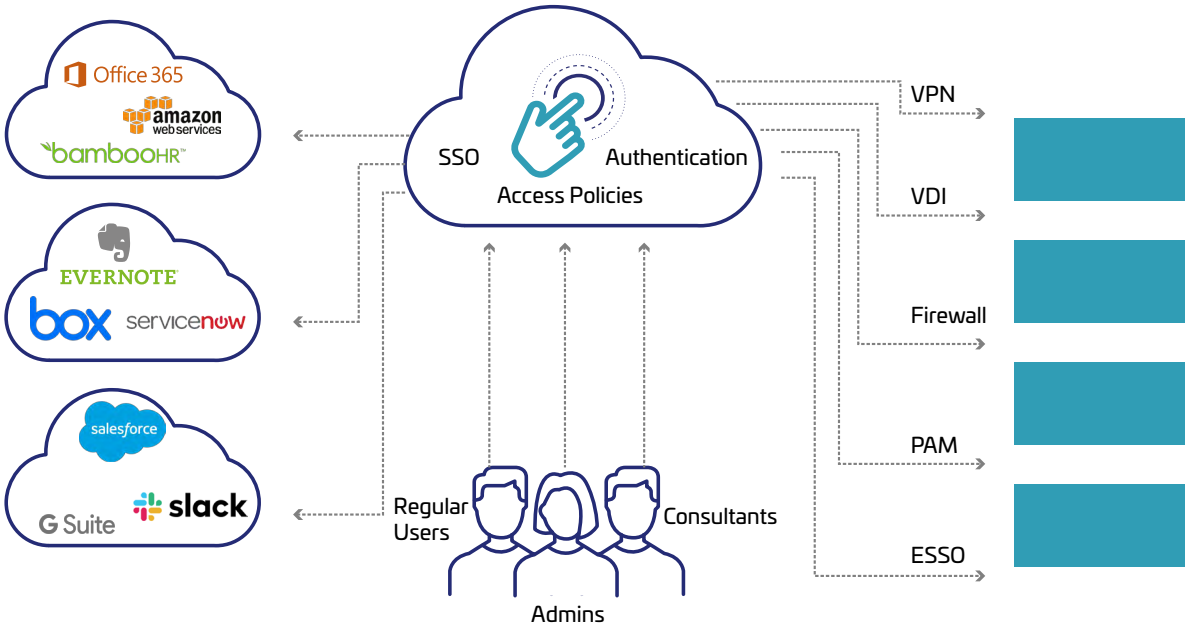
The advisory was published on 1 June 2021; there is no timeline for implementation, as it does not set out any legal obligations per se. However, some of the notices that it supplements (which cover IT more generally and have requirements for each sector) have been in effect for years. The MAS's Technology Risk Management Guidelines, which highlight higher regulatory expectations in terms of security controls and risk governance for IT in general, were shared in January 2021.

Identity and Access Management (IAM)

RISK	MAS Advisory	Thales offering
Item – 11. FIs should implement multi-factor authentication (MFA) for staff.	FIs should implement multi-factor authentication (MFA) for staff with privileges to configure public cloud services through the Cloud Service Providers' (CSPs) megastructure, especially staff with top-level account privileges (e.g., known as "root users" or "subscription owners" for some CSPs).	Thales **SafeNet Trusted Access** supports numerous authentication methods and allows you to leverage authentication strategies already deployed in your organization. The broadest range of authentication methods and form factors, combined with context-based authentication and MFA enhances user convenience and allows you to manage risk by elevating trust only when needed.

RISK	MAS Advisory	Thales offering
Item – 14. FIs using multiple public cloud services may need to centrally manage security policies over the use of different public cloud services and ensure that the policies are consistently enforced.	FIs using multiple public cloud services may need to centrally manage security policies over the use of different public cloud services and ensure that the policies are consistently enforced. FIs may consider adopting solutions such as Cloud Access Security Broker (CASB) or Secure Access Service Edge (SASE) to facilitate policy implementation, enforcement, and timely follow-up on non-compliance issues. CASB solutions manage connections between cloud users and CSPs to enforce security and compliance policies for public cloud services. SASE solutions combine networking and security services, which may include the capabilities of CASB, to enforce security and compliance policies for public cloud services.	Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy - based SSO, universal authentication methods, and MFA, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance. **SafeNet Trusted Access**, Thales's cloud-based access management and authentication service, is the starting point for effective Zero Trust security implementations, meeting the following Zero Trust principles: • Meet a 'verify everywhere, trust no one' stance by enforcing access decisions dynamically at the application access point, irrespective of where the app resides, where users reside, what device users use and network routing. • Adhere to a 'default deny' policy by continuously reassessing and verifying credentials at each log in, even if Single Sign On (SSO) features are enabled.
Item – 18. FIs should also enforce robust IAM to authenticate service requests. FIs should not rely on implicit trusts when granting access (e.g., allow access based on the static IP addresses of requestor).	FIs should also enforce robust IAM to authenticate service requests. FIs should not rely on implicit trusts when granting access (e.g. allow access based on the static IP addresses of requestor).	Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy based SSO, universal authentication methods, and MFA, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance. By leveraging contextual information such as whether the user is logging in from a trusted network or recognized device, access management solutions ensure the most convenient user experience possible — demanding users to step up authentication only in high-risk situations. **SafeNet Trusted Access** uses the OAuth 2.0 and OpenID Connect (OIDC) standard mechanisms to enable you to perform API access management. Instead of client credentials, more secure and time limited access tokens are passed to the API endpoints. In addition, the JSON Web Tokens (JWT) can carry payloads for user context.

Thales IAM solution - SafeNet Trusted Access



Data Protection – Encryption & Key Management

Thales Data Discovery and Classification, Data Encryption/Tokenization and Key Management Solutions

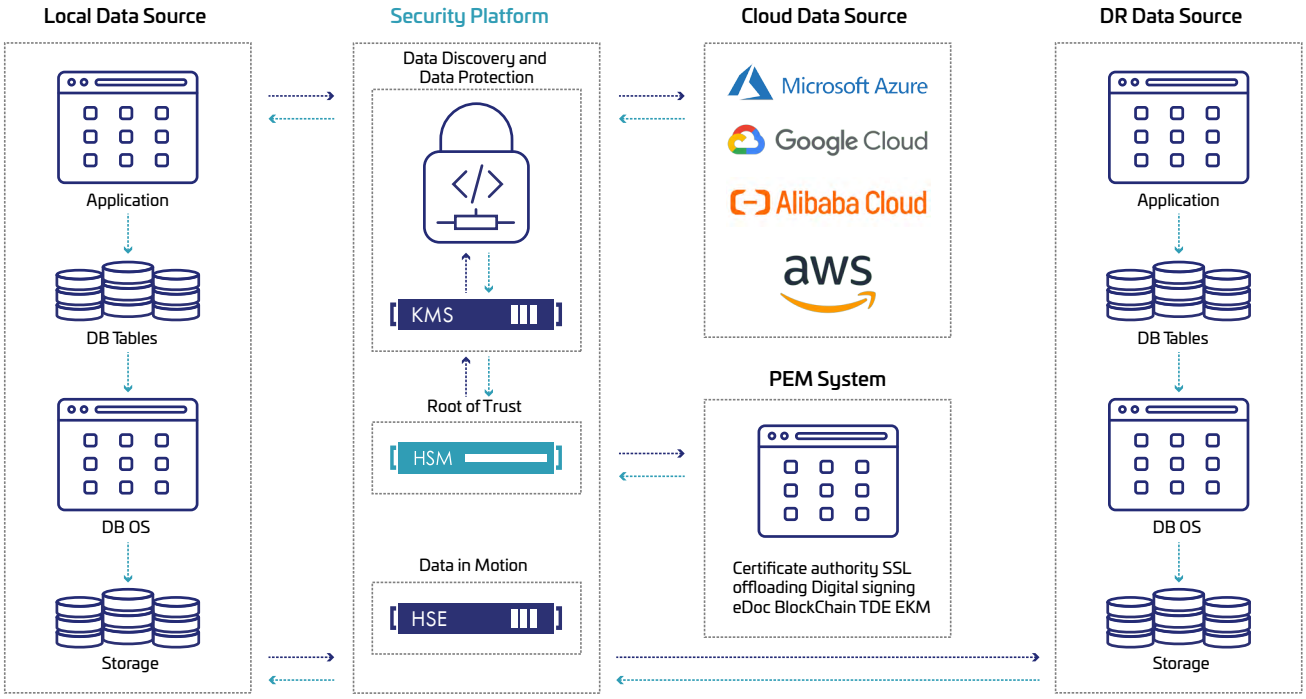


Image above: The Thales Cloud Protection & Licensing solutions in the above images consist of the following components:

√ Protect Data at Rest **√ Protect Data in Motion** **√ Secure Root of Trust**

*Ali Cloud integration planned to complete in Q4 2021

RISK	MAS Advisory	Thales offering
Item – 19. Containers for application adopting microservices architecture.	"Applications that run in a public cloud environment may be packaged in containers, especially for applications adopting a microservices architecture" "FIs should run containers with a similar risk profile together (e.g., based on the criticality of the service or the data that are processed) to minimise risk exposure." "FIs should adopt container-specific security solution for preventing, detecting and responding to container-specific threats"	The CipherTrust platform unifies data discovery, classification, data protection, and provides unprecedented granular access controls, all with centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations, and reduces risk across your business. CipherTrust Transparent Encryption is part of the CipherTrust Data Security Platform. CipherTrust Transparent Encryption Container Security extends CipherTrust Transparent Encryption, letting security teams establish data security controls inside containers. With this extension, you can apply encryption, access control, and data access logging on a per-container basis. Encryption can be applied to data generated and stored locally within the container and to data mounted in the container by network file systems.
Item – 21 (a). For data-at-rest i.e. data in cloud storage	FI may implement additional data object encryption, file encryption, or tokenization, in addition to encryption provided at the platform	Thales offers multiple solutions for data at rest that can coexist with native encryption provided by Cloud Service Provider (CSP). **CipherTrust Transparent Encryption** CipherTrust Transparent Encryption agents are deployed on servers at the file system or volume-level and support both local disks as well as cloud storage environments, such as Amazon S3 and Azure Files **CipherTrust Tokenization** provides tokenization, dynamic data masking for data anonymisation and de-identification in the cloud. **CipherTrust Application Data Protection** provides format preserving or traditional encryption to applications using RESTful APIs. All of the above solutions can be used to provide protection for data at rest in the cloud. **CipherTrust Manager** is the central management point for the CipherTrust Data Security Platform. It manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, supports robust auditing and reporting, and offers developer friendly REST API.

RISK	MAS Advisory	Thales offering
Item – 21(b). For data-in-motion i.e. data that traverses to and from, and within the public cloud	"Data that traverses to and from, and within the public cloud, FIs may implement session encryption or data object encryption in addition to the encryption provided at the platform level"	**Thales High Speed Network Encryption (HSE)** solutions protect any kind of data moving from on premises infrastructure to the cloud. **CipherTrust Tokenization** With CipherTrust Tokenization, Organization's can tokenize data and maintain control and compliance when moving data to the cloud or big data environments. Cloud providers have no access to token vaults or any of the keys associated with tokenization root of trust.
Item – 22. Key management and data protection before moving to cloud.	"FIs should consider adopting cryptographic key management strategies that accord them a high level of control and protection over cryptographic keys used for encrypting sensitive data." "Two ways which FIs can retain greater control of the keys are "Bring-Your-Own-Key" (BYOK) and "Bring-Your-Own-Encryption" (BYOE)." "BYOK allows FIs to retain control and management of cryptographic keys that would be uploaded to the cloud to perform data encryption." "In BYOE, data is encrypted before it enters the cloud and the keys are not transferred to the cloud."	**Bring Your Own Key (BYOK)** The CipherTrust Data SecurityPlatform offers advanced encryption and centralized key management solutions that enable organizations to safely store sensitive data in the cloud. The platform offers advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor encryption lock-in and ensure the data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management. Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using the CipherTrust Cloud Key Manager. The CipherTrust Cloud Key Manager supports Bring Your Own Key (BYOK) use-cases across multiple cloud infrastructures and SaaS applications. With the CipherTrust Data Security Platform, the strongest safeguards protect an enterprise's sensitive data and applications in the cloud, helping the organization meet compliance requirements and gain greater control over data, wherever it is created, used, or stored. **Thales Cipher Trust Cloud Key Manager** combines support for cloud provider BYOK APIs, cloud key management automation, and key usage logging and reporting, to provide cloud consumers with a cloud key management service that delivers strong controls over encryption key life cycles for data encrypted by cloud services. **Bring Your Own Encryption (BYOE)** **CipherTrust Transparent Encryption** Provides transparent encryption and access control for data residing in Amazon S3 and Azure Files **CipherTrust Tokenization** tokenizes the data before it is migrated to the cloud in obfuscated form to protect the data from any breach.

RISK	MAS Advisory	Thales offering
Item – 23. Crypto key protection	" To secure cryptographic keys used for encrypting sensitive data, FI may consider generating, storing and managing the keys in a hardware security module (HSM) and hosting the HSM in an environment that the FI has a higher degree of control over (e.g. FI's own on-premise IT infrastructure) rather than with the Cloud Service Provider (CSP)."	**Thales Luna Hardware Security Modules (HSM)** or **CipherTrust Mnager (CM)** should be used for key generation, storage and end to end key lifecycle management. This allows organisations to have a greater degree of control and ownership over the crypto keys rather than with the Cloud Service Provider (CSP).
Item 24. Risk associated to cryptographic keys managed by the Cloud Service Provider (CSP)	"For cryptographic keys managed by CSPs, FIs should ensure that the CSPs' cryptographic key management policy, standards and procedures are adequate to protect the keys from unauthorised access, usage and disclosure throughout the cryptographic key management life cycle. This includes key generation, distribution, installation, renewal, revocation, recovery and expiry."	**Thales Cipher Trust Cloud Key Manager (CCKM)** is a unique platform that leverages the Bring Your Own Key (BYOK) API to manage multiple cloud providers from a single interface. It provides auditing of key, strong key generation, end to end key lifecycle management along automatic key rotation, recovery and key revocation feature that is not available by any cloud provider's managed Key Management System (KMS).
Item 34 – 36. Vendor lock in	"To mitigate Cloud Service Provider (CSP) concentration risks, FIs may consider implementing vendor diversity measures such as implementing a multi-cloud strategy" "To mitigate the risks of vendor lock-in, FIs may adopt cloud portability or interoperability solutions"	Multiple Cloud Providers offer their encryption services as a convenience to their customers. A growing number of cloud providers offer "Bring Your Own Key" (BYOK) services. The challenge of BYOK and cloud key management depends on the number of clouds and keys organisations need to manage. **CipherTrust Cloud Key Manager** combines support for cloud provider BYOK service, cloud key management automation, and key usage logging and reporting, to provide cloud consumers with strong controls over encryption key life cycles for data encrypted by a cloud service provider. Thales **CipherTrust Transparent Encryption (CTE)** and **CipherTrust Tokenization** offers advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor encryption lock-in and ensure the data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management.

Thales tools for compliance with data security regulations and standards

In our review of Singapore's advisory on addressing the technology and cyber security risks associated with public cloud adoption, we note where and how Thales Cloud Protection & Licensing (CPL) can help organisations comply and recommend specific products. In this section, we summarize those products and provide links to more information.

Data security measures called for in virtually all regulations and standards.

PKI

Create a Public Key Infrastructure to secure access to apps, protect your software from tampering, prevent unauthorized devices, and sign code & documents.

Big Data Security

Create isolation in your data lakes, mask sensitive data, and control admin users for security and compliance.

Data Security

Thales provides data security through encryption, key management, access control and security intelligence across devices, processes, platforms and environments.

Payment Security

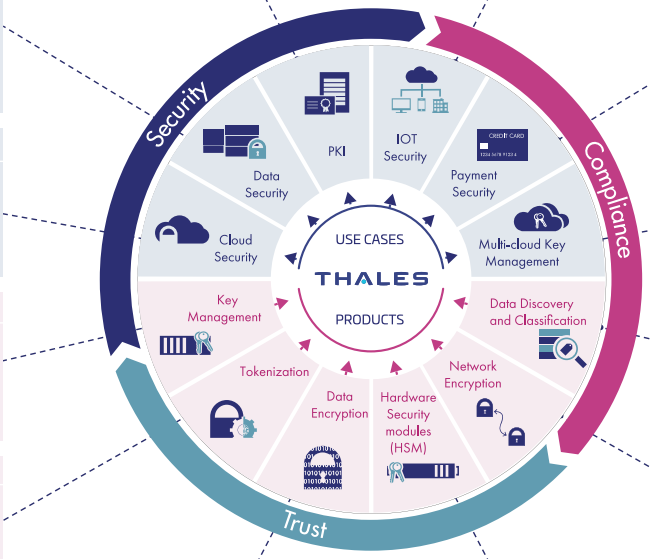
Enable compliance,reduce risks, and increase operational efficiency for payment transactions across the globe.

Cloud Security

Secure your digital transformation with industry-leading encryption, key management, HSM and access management solutions from Thales.

Multicloud Key Management

Multicloud Lifecycle Key Management enables your team to efficiently control and report on BYOK and hybrid cloud key usage.



Key Management

Thales Data Security Manager (DSM) provisions and manages keys for Thales Data Security Platform and also manages keys and certificates for third-party devices.

Application Crypto

Streamline secure development through APIs for tokenisation, encryption and other cryptographic functions.

Access Management

Prevent breaches, move security to the cloud and simplify compliance with Thales Access Management and Authentication solutions.

WAN Encryption

Proven high-assurance network security for your sensitive data, real-time video and voice, on the move between data centers and sites.

Transparent Encryption

Encrypts, controls access to data and provides data access audit logging without impacting applications, databases or infrastructure - wherever servers are deployed. This could be smoother, do you want to communicate that Transparent Encryption can be used in any server, regardless of the cloud provider?

Hardware Security Modules

A hardware security module (HSM) is a high-assurance crypto processor that provides a root of trust. Thales leads the industry in General Purpose, Payment and Cloud HSM solutions.

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.

THALES

Building a future we can all trust

Contact us

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

> cpl.thalesgroup.com <

© Thales - August 2021 • EH v5