

# AWS User Guide to Financial Services Regulations & Guidelines in Singapore

**First Published July 2017**

*Updated January 3, 2022*



## Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

© 2022 Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Contents

- About this guide ..... 1
- Security of the cloud .....4
  - AWS compliance programs .....5
  - AWS Artifact .....7
- AWS Regions .....7
- MAS Guidelines on Outsourcing.....8
  - Assessment of service providers .....8
  - Cloud computing .....11
  - Outsourcing agreements.....15
  - Audit and inspection .....16
- MAS Technology Risk Management Guidelines .....17
- Notice 655 on Cyber Hygiene .....20
- ABS Cloud Computing Implementation Guide 2.0 .....23
  - Key controls.....23
- Next steps .....26
- Conclusion .....28
- Additional resources .....28
- Contributors .....30
- Document revisions .....30

# Abstract

This document provides information to help regulated financial institutions (FIs) operating in Singapore as they accelerate their use of Amazon Web Services (AWS) Cloud services.

## About this guide

This document provides information to assist banks and financial services institutions in Singapore regulated by the Monetary Authority of Singapore (MAS) as they adopt and accelerate their use of the AWS Cloud.

This guide:

- Describes the respective roles that the customer and AWS each play in managing and securing the cloud environment;
- Provides an overview of the regulatory requirements and guidance that financial institutions can consider when using AWS; and
- Provides additional resources that financial institutions can use to help them design and architect their AWS environment to be secure and meet regulatory expectations.

The Monetary Authority of Singapore (MAS) *Guidelines on Outsourcing* for financial institutions (FIs) acknowledges that FIs can leverage cloud services to enhance their operations and reap the benefit of the scale, standardization, and security of the cloud. The MAS *Guidelines on Outsourcing* instruct FIs to perform due diligence and apply sound governance and risk management practices to their use of cloud services.

The following sections provide considerations for FIs as they assess their responsibilities related to the following guidelines:

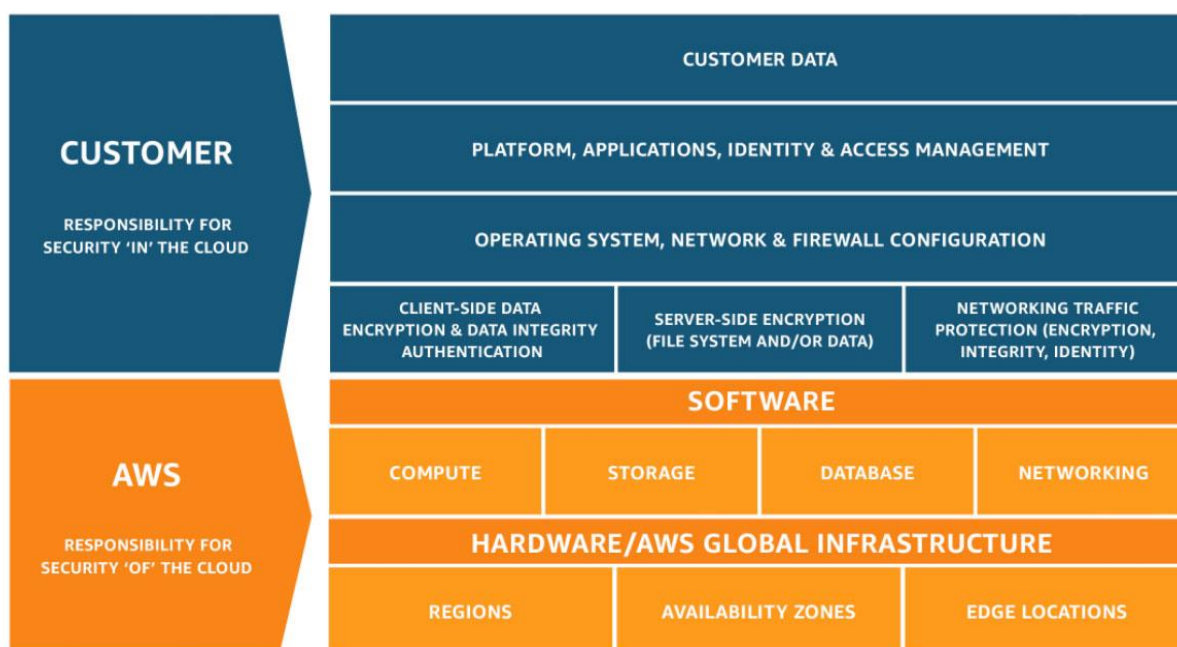
- **MAS Guidelines on Outsourcing** – The *Guidelines on Outsourcing* provide expanded guidance to the industry on prudent risk management practices for outsourcing, including cloud services.
- **MAS Technology Risk Management (TRM) Guidelines** – These include guidance for a high level of reliability, availability, and recoverability of critical IT systems, and for FIs to implement IT controls to protect customer information from unauthorized access or disclosure.
- **Notice 655 on Cyber Hygiene**: – This notice sets out cyber security requirements on securing administrative accounts, applying security patching, establishing baseline security standards, deploying network security devices, implementing anti-malware measures and strengthening user authentication.

- Association of Banks in Singapore (ABS) Cloud Computing Implementation Guide 2.0** – This guide is intended to assist FIs in further understanding approaches to due diligence, vendor management, and key controls that should be implemented in cloud outsourcing arrangements.

Taken together, FIs can use this information for their due diligence and to assess how to implement an appropriate information security, risk management, and governance program for their use of AWS.

## Security and the Shared Responsibility Model

Before exploring the requirements included in the various guidelines, it is important that FIs understand the AWS Shared Responsibility Model.



*AWS Shared Security Responsibility Model*

AWS operates, manages, and controls the IT components from the host operating system and virtualization layer, down to the physical security of the facilities in which the services operate. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS-provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared

responsibility also provides the flexibility and customer control that permits the deployment.

As shown in the preceding chart, this differentiation of responsibility is commonly referred to as Security “of” the Cloud versus Security “in” the Cloud. Customers should carefully consider the services they choose, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations.

When using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

- The content that customers choose to store on AWS
- The AWS services that are used with the content
- The country where the content is stored
- The format and structure of that content and whether it is masked, anonymized, or encrypted
- How the data is encrypted and where the keys are stored
- Who has access to that content and how those access rights are granted, managed, and revoked

It is possible to enhance security and meet more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection and prevention, and encryption. AWS provides tools and information to assist customers in their efforts to account for and validate whether controls are operating effectively in their extended IT environment. For more information, refer to the AWS Compliance Center at <http://aws.amazon.com/compliance>.

For more information on the Shared Responsibility Model, and its implications for the storage and processing of personal data and other content using AWS, refer to [Using AWS in the Context of Singapore Privacy Considerations](#).

## Security of the cloud

To provide security of the cloud, AWS environments are nearly continuously audited, and the infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and verticals. Customers can use these certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications. The AWS compliance program is based on the following actions:

- **Validate** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment includes policies, processes, and control activities that leverage various aspects of the AWS overall control environment.

The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of our control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that it can implement, and to better assist customers with managing their control environment.

- **Demonstrate** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS. Customers can leverage this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.
- **Monitor** that AWS maintains compliance with global standards and best practices, through the use of thousands of security control requirements.

## AWS compliance programs

AWS has obtained certifications and independent, third-party attestations for a variety of industry-specific workloads. The following are of particular importance to FIs:

- **ISO 27001** – ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, refer to <https://aws.amazon.com/compliance/iso-27001-faqs/>.
- **ISO 27017** – ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional information security controls and implementation guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, refer to <https://aws.amazon.com/compliance/iso-27017-faqs/>.
- **ISO 27018** – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements, which is not addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, refer to <https://aws.amazon.com/compliance/iso-27018-faqs/>.
- **ISO 9001** – ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. The key to the ongoing certification under this standard is establishing, maintaining and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner in which AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, refer to <https://aws.amazon.com/compliance/iso-9001-faqs/>.

- **MTCS Level 3** – Multi-Tier Cloud Security (MTCS) is an operational Singapore security management Standard (SPRING SS 584:2013), based on ISO 27001/02 Information Security Management System (ISMS) standards. The key to the ongoing three-year certification under this standard is the effective management of a rigorous security program and annual monitoring by an MTCS Certifying Body (CB). The Information Security Management System (ISMS) required under this standard defines how AWS perpetually manages security in a holistic, comprehensive way. For more information, refer to <https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/>.
- **Outsourced Service Provider's Audit Report (OSPAR)** – The ABS Guidelines recommend that Singapore banks select outsourced service providers that meet the controls set out in the ABS Guidelines, which can be demonstrated through an OSPAR. An OSPAR attestation involves an external audit of the service provider's controls against the criteria specified in the ABS Guidelines. For more information, refer to <https://aws.amazon.com/compliance/OSPAR/>.
- **PCI DSS Level 1** – The Payment Card Industry Data Security Standard (also known as PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, refer to <https://aws.amazon.com/compliance/pci-dss-level-1-faqs/>.
- **SOC** – AWS Service Organization Control (SOC) Reports are independent, third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls established to support operations and compliance. For more information, refer to <https://aws.amazon.com/compliance/soc-faqs/>.

There are three types of AWS SOC Reports:

- **SOC 1** – Provides information about the AWS control environment that might be relevant to a customer's internal controls over financial reporting as well as information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).

- **SOC 2** – Provides customers and their service users that have a business need with an independent assessment of the AWS control environment that is relevant to system security, availability, and confidentiality.
- **SOC 3** – Provides customers and their service users that have a business need with an independent assessment of the AWS control environment that is relevant to system security, availability, and confidentiality, without disclosing AWS internal information.

For more information about the other certifications and attestations from AWS, refer to the AWS Compliance Center at <https://aws.amazon.com/compliance/>.

For a description of general security controls and service-specific security from AWS, refer to [AWS Overview of Security Processes](#).

## AWS Artifact

Customers can review and download reports and details about more than 2,500 security controls by using AWS Artifact, the self-service audit artifact retrieval portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, the AWS MAS Technology Risk Management Workbook, and certifications from accreditation bodies across geographies and compliance verticals.

## AWS Regions

The AWS Cloud infrastructure is built around Regions and Availability Zones. A Region is a physical location in the world with multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, all housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases which are more highly available, fault tolerant, and scalable than would be possible from a single data center.

For additional information on AWS Regions and Availability Zones, refer to <https://aws.amazon.com/about-aws/global-infrastructure/>.

## MAS Guidelines on Outsourcing

The MAS *Guidelines on Outsourcing* provide guidance and recommendations on prudent risk management practices for outsourcing, including the use of cloud services by FIs. FIs that use the cloud are expected to carry out due diligence, evaluate and address risks, and enter into appropriate outsourcing agreements. The *Guidelines on Outsourcing* expressly state that the extent and degree to which an FI implements the specific guidance therein should be commensurate with the nature of risks in, and materiality of, the outsourcing. FIs should also demonstrate their observance of the guidelines to MAS through the submission of an outsourcing register to MAS annually, or on request.

A full analysis of the *Guidelines on Outsourcing* is beyond the scope of this document. However, the following information includes the considerations in the Guidelines that AWS most frequently encounters in interactions with Singapore's FIs.

### Assessment of service providers

Section 5.4.3 of the *Guidelines on Outsourcing* includes a partial list of topics that should be evaluated in the course of due diligence when an FI is considering an outsourcing arrangement, such as use of the cloud. The following table includes considerations for each component of section 5.4.3 of the MAS *Outsourcing Guidelines*.

*Table 1 – Considerations for section 5.4.3 of the MAS Outsourcing Guidelines*

| Due diligence requirement                                                                                           | AWS response                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.4.3 (a) Experience and capability to implement and support the outsourcing arrangement over the contracted period | Since 2006, AWS has provided flexible, scalable, and secure IT infrastructure to businesses of all sizes around the world. AWS continues to grow and scale, which allows us to provide new services that help millions of active customers.                                                                               |
| 5.4.3 (b) Financial strength and resources                                                                          | The financial statements of Amazon.com, Inc. include sales and income information from AWS, permitting assessment of its financial position, and the ability to service its debts and/or liabilities. These financial statements are available from the SEC or at the <a href="#">Amazon Investor Relations website</a> . |

| Due diligence requirement                                                                                        | AWS response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.4.3 (c) Corporate governance, business reputation and culture, compliance, and pending or potential litigation | <p>AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. Maintaining customer trust and confidence is of the utmost importance to AWS.</p> <p>AWS performs a nearly continuous risk assessment process to identify, evaluate, and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. The AWS risk management team monitors and escalates risks on a nearly continuous basis, performing risk assessments on newly implemented controls at least every six months.</p> <p>For additional information, see these AWS Audit Reports: SOC 2, PCI DSS, ISO 27001, ISO 27017.</p> <p>Amazon.com has a Code of Business Conduct and Ethics, available at the Amazon Investor Relations website, which encompasses considerations such as compliance with laws, conflicts of interest, bribery, discrimination and harassment, health and safety, recordkeeping, and financial integrity.</p> <p>Information on legal proceedings can be found within the Amazon.com, Inc. Form 10-K filing, available at the Amazon Investor Relations website or the website of the US Securities and Exchange Commission.</p> |
| 5.4.3 (d) Security and internal controls, audit coverage, reporting and monitoring environment                   | <p>AWS management re-evaluates the security program at least biannually. This process includes risk assessment and implementation of appropriate measures designed to address those risks.</p> <p>AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. To learn more about each of the audit programs leveraged by AWS, refer to the <a href="#">AWS Compliance Programs</a>.</p> <p>Compliance reports from these assessments are made available through <a href="#">AWS Artifact</a> to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and Regions assessed, as well the assessor's attestation of compliance. Customers can also leverage reports and certifications available through AWS Artifact to evaluate vendors or suppliers according to their requirements.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Due diligence requirement                                                                                                                                               | AWS response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.4.3 (e) Risk management framework and capabilities, including technology risk management and business continuity management in respect of the outsourcing arrangement | AWS performs a nearly continuous risk assessment process to identify, evaluate and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. AWS monitors and escalates risks on a nearly continuous basis, regularly performing risk assessments on newly implemented controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 5.4.3 (f) Disaster recovery arrangements and disaster recovery track record                                                                                             | <p>The AWS Business Continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. This plan has been developed to recover and reconstitute AWS using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach ensures that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and omissions.</p> <p>AWS maintains a ubiquitous security control environment across all Regions. Each data center is built to physical, environmental, and security standards in an active-active configuration, employing an n+1 redundancy model designed to ensure system availability in the event of component failure.</p> <p>Components (N) have at least one independent backup component (+1), so the backup component is active in the operation even if all other components are fully functional. In order to reduce single points of failure, this model is applied throughout AWS, including network and data center implementation. All data centers are online and serving traffic; no data center is <i>cold</i>. In case of failure, there is sufficient capacity to enable traffic to be load balanced to the remaining sites.</p> <p>Customers are responsible for properly implementing contingency planning, training, and testing for their systems hosted on AWS. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic Regions as well as across multiple Availability Zones within each Region. Each Availability Zone is designed as an independent failure zone. In the case of failure, automated processes move customer data traffic away from the affected area. This means that Availability Zones are typically physically separated within a metropolitan region and are in different flood plains.</p> |

| Due diligence requirement                                                                                                                                                                                                                                                                                           | AWS response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                     | Customers use AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS Cloud supports many popular disaster recovery (DR) architectures, from <i>pilot light</i> environments that are ready to scale up at a moment's notice to <i>hot standby</i> environments that enable rapid failover.                                                                                                                                                                                                                                                                                                                  |
| 5.4.3 (g) Reliance on and success in dealing with subcontractors                                                                                                                                                                                                                                                    | AWS has a program in place for selecting vendors and periodically evaluating vendor performance and compliance with contractual obligations. AWS implements policies and controls to monitor access to resources that process or store customer content. Vendors and third parties with restricted access, that engage in business with Amazon, are subject to confidentiality commitments as part of their agreements with Amazon. To monitor subcontractor access year-round, refer to <a href="https://aws.amazon.com/compliance/third-party-access/">https://aws.amazon.com/compliance/third-party-access/</a> .                                                                                     |
| 5.4.3 (h) Insurance coverage                                                                                                                                                                                                                                                                                        | Amazon's Memorandum of Insurance is available on the <a href="#">Amazon Investor Relations website</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 5.4.3 (i) External environment (such as the political, economic, social and legal environment of the jurisdiction in which the service provider operates);<br>5.4.3 (j) Ability to comply with applicable laws and regulations and track record in relation to its compliance with applicable laws and regulations. | AWS complies with applicable federal, state, and local laws, statutes, ordinances, and regulations concerning security, privacy, and data protection of AWS services, which helps to minimize the risk of accidental or unauthorized access or disclosure of customer content.<br>AWS formally tracks and monitors its regulatory and contractual agreements and obligations. AWS has performed and maintains the following activities: <ul style="list-style-type: none"> <li>• Identified applicable laws and regulations for each of the jurisdictions in which AWS operates.</li> <li>• Documented and maintains all statutory, regulatory, and contractual requirements relevant to AWS.</li> </ul> |

## Cloud computing

The updated MAS *Guidelines on Outsourcing* include a chapter on cloud computing. MAS notes that cloud services can potentially offer many advantages including the following:

- Economies of scale
- Cost-savings

- Access to quality system administration
- Operations that adhere to uniform security standards and best practices
- Flexibility and agility for institutions to scale up or pare down on computing resources quickly as usage requirements change
- Enhance system resilience during location-specific disasters or disruptions

MAS also clarified that it considers cloud computing a form of outsourcing, and that the types of risks arising from using the cloud to FIs are not distinct from those of other forms of outsourcing arrangements. FIs are still expected to perform the necessary due diligence and apply sound governance and risk management practices, in a similar manner that the FI would for any other outsourcing arrangement.

Section 6 of the *Guidelines on Outsourcing* outlines a partial list of specific risks that should be evaluated and addressed by an FI that uses cloud services. The following table includes considerations relevant to each risk mentioned in paragraph 6.7 of the *Guidelines*.

*Table 2 — Considerations relevant to paragraph 6.7 of the Outsourcing Guidelines*

| Risk area                                   | AWS controls                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data access, confidentiality, and integrity | <p>AWS gives customers ownership and control over their customer content by design through simple, but powerful tools that allow customers to determine where to store their customer content, secure their customer content in transit or at rest, and manage access to AWS services and resources for their users. AWS implements responsible and sophisticated technical and physical controls designed to prevent unauthorized access to or disclosure of customer content.</p> <p>AWS seeks to maintain data integrity through all phases including transmission, storage, and processing. AWS treats all customer data and associated assets as highly confidential. AWS services are content agnostic, which means that they offer the same high level of security to all customers, regardless of the type of content being stored. AWS is vigilant about customers' security and has implemented sophisticated technical and physical measures against unauthorized access. AWS has no insight as to what type of content the customer chooses to store in AWS, and the customer retains complete control of how they choose to classify their content, where it is stored, and how it is used and protected from disclosure.</p> |

| Risk area      | AWS controls                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <p>Customer-provided data is validated for integrity, and corrupted or tampered data is not written to storage. <a href="#">Amazon Simple Storage Service</a> (Amazon S3) uses checksums internally to confirm the continued integrity of data in transit within the system and at rest. Amazon S3 provides a facility for customers to send checksums with the data transmitted to the service. The service validates the checksum upon receipt of the data to determine that no corruption occurred in transit. Regardless of whether a checksum is sent with an object to Amazon S3, the service uses checksums internally to confirm the continued integrity of data in transit within the system and at rest. When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy. External access to data stored in Amazon S3 is logged and the logs are retained for at least 90 days, including relevant access request information, such as the data accessor IP address, object, and operation.</p> <p>For more information, see the following AWS Audit Reports: SOC 1, SOC 2, PCI DSS, ISO 27001, ISO 27017</p> |
| Sovereignty    | <p>AWS customers choose the physical Region in which their data and servers are located. AWS does not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or a binding order of a governmental body. For more information, refer to <a href="#">Using AWS in the context of Singapore Privacy Considerations</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Recoverability | <p>The Amazon infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.</p> <p>AWS provides customers with the flexibility to place instances and store data within multiple geographic Regions, as well as across multiple Availability Zones within each Region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region, and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete, non-interruptible power supply (UPS) and onsite backup generation facilities, they are each fed through different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers.</p>                                                                                                                                                                    |

| Risk area             | AWS controls                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regulatory compliance | <p>AWS formally tracks and monitors its regulatory and contractual agreements and obligations. To do so, AWS has performed and maintains the following activities:</p> <ul style="list-style-type: none"><li>• Identified applicable laws and regulations for each of the jurisdictions in which AWS operates</li><li>• Documented and maintains all statutory, regulatory, and contractual requirements relevant to AWS</li><li>• Categorized records into types with details of retention periods and type of storage media through the Data Classification Policy</li><li>• Informed and trained personnel (employees, contractors, third-party users) that must be made aware of compliance policies to protect sensitive AWS information (such as intellectual property rights and AWS records) through the Data Handling Policy</li><li>• Monitors the use of AWS facilities for unauthorized activities with a process in place to enforce appropriate disciplinary action</li></ul> <p>AWS maintains relationships with outside parties to monitor business and regulatory requirements. Should a new security directive be issued, AWS has documented plans in place to implement that directive within designated time frames.</p> <p>For more information, see the following AWS Audit Reports: SOC 1, SOC 2, PCI DSS, ISO 27001, ISO 27017</p> |
| Auditing              | <p>Enabling our customers to protect the confidentiality, integrity, and availability of systems and content is of the utmost importance to AWS, as is maintaining customer trust and confidence. To make sure these standards are met, AWS has established a formal audit program to validate the implementation and effectiveness of the AWS control environment.</p> <p>The AWS audit program includes internal audits and third-party accreditation audits. The objective of these audits is to evaluate the operating effectiveness of the AWS control environment. Internal audits are planned and performed periodically. Audits by third-party accreditation are conducted to review the continued performance of AWS against standards-based criteria, and to identify general improvement opportunities.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Risk area                    | AWS controls                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | <p>Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and Regions assessed, as well as the assessor's attestation of compliance. Customers can also leverage reports and certifications available through AWS Artifact to evaluate vendors or suppliers according to their requirements.</p> <p>Some of our key audit programs and certifications are described in the <a href="#">AWS compliance programs</a> section of this document. For a full list of audits, certifications, and attestations, refer to the <a href="#">AWS Compliance Center</a>.</p>                                                                                                                                                                                                                                                                                                                    |
| Segregation of customer data | <p>Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customers maintain full control over who has access to their data. Services which provide virtualized operational environments to customers (for example, EC2) are designed to ensure that customers are segregated from one another and prevent cross-tenant privilege escalation and information disclosure via hypervisors and instance isolation.</p> <p>Customers can also use Amazon Virtual Private Cloud (VPC) which gives them complete control over their virtual networking environment, including resource placement, connectivity, and security. The first step is to create your VPC. Then you can add resources to it, such as Amazon Elastic Compute Cloud (EC2) and Amazon Relational Database Service (RDS) instances. Finally, you can define how your VPCs communicate with each other across accounts, Availability Zones (AZs), or Regions.</p> |

## Outsourcing agreements

Section 5.5 of the *Guidelines on Outsourcing* clarifies that contractual terms and conditions governing the use of the cloud should be defined in written agreements. MAS expects such agreements to address, at the least, the scope of the outsourcing arrangement; performance, operational, internal control, and risk management standards; confidentiality and security; business continuity management; monitoring, and control; audit and inspection; notification of adverse developments; dispute resolution; default termination and early exit; sub-contracting; and applicable laws.

AWS customers have the option to enroll in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs. AWS also provides an introductory guide to help Singapore's FIs assess

the AWS Enterprise Agreement against the *Guidelines on Outsourcing*. For more information about AWS Enterprise Agreements, contact your AWS representative.

## Audit and inspection

The *Guidelines on Outsourcing* clarify that an FI's outsourcing arrangements should not interfere with the ability of the FI to effectively manage its business activities or impede MAS in carrying out its supervisory functions and objectives.

Customers retain ownership and control of their content when they use AWS services, and do not cede that ownership and control of their content to AWS. Customers have complete control over which services they use and whom they allow to access their content and services, including what credentials are required. Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use, and how they use them.

AWS does not change customer configuration settings, because these settings are determined and controlled by the customer. AWS customers have the complete freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS enables and empowers the customer to decide when and how security measures are implemented in the cloud, in accordance with each customer's business needs.

For example, if a higher availability architecture is required to protect customer content, the customer can add redundant systems, backups, locations, and network uplinks to create a more resilient, high-availability architecture. If restricted access to customer content is required, AWS enables the customer to implement access rights management controls, both on a systems level and through encryption on a data level. For more information, refer to [Using AWS in the Context of Singapore Privacy Considerations](#).

The *Guidelines on Outsourcing* also require FIs to have access to audit reports and findings made on service providers, whether produced by the service provider's or its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractor, in relation to the outsourcing agreement.

Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2, and 3 reports, ISO 27001, 27017 and 27018 certifications, and PCI DSS

compliance reports. These reports and certifications are produced by independent, third-party auditors, and attest to the design and operating effectiveness of AWS security controls.

For more information about how AWS approaches audits and inspections, and how these requirements may be addressed in an Enterprise Agreement with AWS, contact your AWS representative.

## MAS Technology Risk Management Guidelines

The MAS Technology Risk Management (TRM) Guidelines define risk management principles and best practice standards to guide FIs in the following:

- Establishing a sound and robust technology risk management framework
- Strengthening system security, reliability, resiliency, and recoverability
- Deploying strong authentication to protect customer data, transactions, and systems

AWS has produced a MAS TRM Guidelines Workbook that maps AWS security and compliance controls (*OF the cloud*) and best practice guidance provided by the [AWS Well-Architected Framework](#) (*IN the cloud*) to the requirements within the MAS TRM Guidelines. Where applicable, under the AWS Shared Responsibility Model, the workbook provides supporting details and references to assist FIs when they adapt the MAS TRM Guidelines for their workloads on AWS.

The [Well-Architected Framework](#) helps you understand the pros and cons of decisions you make while building systems on AWS. By using the framework, you learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement. The process for reviewing an architecture is a constructive conversation about architectural decisions, and is not an audit mechanism. AWS believes that having well-architected systems greatly increases the likelihood of business success.

AWS Solutions Architects have years of experience architecting solutions across a wide variety of business verticals and use cases. They have helped design and review thousands of customers' architectures on AWS. From this experience, they have identified best practices and core strategies for architecting systems in the cloud.

The AWS Well-Architected Framework documents a set of foundational questions that allow you to understand whether a specific architecture aligns well with cloud best practices. The Framework provides a consistent approach to evaluating systems against the qualities you expect from modern, cloud-based systems, and the remediation that would be required to achieve those qualities. As AWS continues to evolve, and continues to learn more from working with customers, the definition of well-architected will continue to be refined.

The Framework is intended for those in technology roles, such as chief technology officers (CTOs), architects, developers, and operations team members. It describes AWS best practices and strategies to use when designing and operating a cloud workload, and provides links to further implementation details and architectural patterns. For more information, refer to the [AWS Well-Architected page](#).

The following table excerpt shows an example of the response from AWS to guideline 9.1.5 in the TRM Guidelines:

*Table 3 — Response from AWS to guideline 9.1.5 in the TRM Guidelines*

| Requirement                                                                                                                                                             | Responsibility | AWS supporting information                                                                 | Additional information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.1.5 Multi-factor authentication should be implemented for users with access to sensitive system functions to safeguard the systems and data from unauthorized access. | AWS            | AWS Control Objective:<br><br>Governance and Risk Management - Shared Responsibility Model | Security and compliance is a shared responsibility between AWS and the customer. AWS is responsible for the security and compliance 'of' the cloud, and implements security controls to secure the underlying infrastructure that runs the AWS services and hosts and connects customer resources. AWS customers are responsible for security 'in' the cloud and should determine, design and implement the security controls needed based on their security and compliance needs and AWS services they select. The customer responsibility will be determined by the AWS services that a customer selects. AWS provides customers with best practices on how to secure their resources within the AWS service's documentation at <a href="http://docs.aws.amazon.com/">http://docs.aws.amazon.com/</a> . |

| Requirement                                                                                                                                                                    | Responsibility | AWS supporting information                                                                                                                                 | Additional information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                | AWS            | <p>AWS Control Objective:</p> <p>Identity and Access Management - Administrative Access</p>                                                                | <p>Amazon personnel with a business need to access the management plane are required to first use multi-factor authentication to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane; such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked.</p> |
| <p>9.1.5 Multi-factor authentication should be implemented for users with access to sensitive system functions to safeguard the systems and data from unauthorized access.</p> | Customer       | <p>Well-Architected - Question/Best Practice:</p> <p>SEC-2 - How do you manage authentication for people and machines? - Use strong sign-in mechanisms</p> | <p>Enforce minimum password length, and educate users to avoid common or re-used passwords.</p> <p>Enforce multi-factor authentication (MFA) with software or hardware mechanisms to provide an additional layer.</p>                                                                                                                                                                                                                                                                                                        |

FIs can create an AWS account at [AWS Artifact](#) and get a copy of the AWS MAS TRM Workbook from the [AWS Artifact portal](#) after logging in.

FIs should review responses from AWS in the AWS MAS TRM Workbook, and enrich them with the FI’s own company-wide controls. For example, section 3 of the MAS TRM Guidelines discusses the oversight of technology risk by the board of directors and senior management. This is a principle that is likely to apply company-wide, is not specific to cloud or particular applications, and can only be addressed by the FI. The AWS MAS TRM Workbook also positions FIs to more clearly consider whether and how

to add extra or supplementary technology risk controls that are specific to line of businesses or application teams, or the FI’s particular needs.

## Notice 655 on Cyber Hygiene

The Notice 655 on Cyber Hygiene applies to all banks in Singapore. It sets out cyber security requirements on securing administrative accounts, applying security patching, establishing baseline security standards, deploying network security devices, implementing anti-malware measures and strengthening user authentication.

AWS has produced the AWS Workbook for MAS Notice 655 on Cyber Hygiene that maps AWS security and compliance controls (*OF the cloud*) and best practice guidance provided by the [AWS Well-Architected Framework](#) (*IN the cloud*) to the requirements within the Notice 655. Where applicable, under the AWS Shared Responsibility Model, the workbook provides supporting details and references to assist FIs when they adapt the Notice 655 on Cyber Hygiene for their workloads on AWS.

The following table excerpt shows an example of the response from AWS to Cyber Hygiene Practice 4.3 in the Notice 655 for Cyber hygiene:

Table 4 — Response from AWS to Cyber Hygiene Practice 4.3

| Requirement                                          | Responsibility | AWS supporting information                                                    | Additional information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------|----------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.3 Security Standards - IV. Cyber Hygiene Practices | AWS            | AWS Control Objective: Governance and Risk Management - Baseline Requirements | <p>AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers’ systems and content. Maintaining customer trust and confidence is of the utmost importance to AWS.</p> <p>AWS complies with applicable federal, state, and local laws, statutes, ordinances, and regulations concerning security, privacy and data protection of AWS services, which helps to minimize the risk of accidental or unauthorized access or disclosure of customer content.</p> |

| Requirement                                          | Responsibility | AWS supporting information                                                                        | Additional information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------|----------------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.3 Security Standards - IV. Cyber Hygiene Practices | AWS            | <p>AWS Control Objective:</p> <p>Governance and Risk Management - Security Control Framework</p>  | <p>AWS has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems and content. AWS maintains a broad range of industry and geography-specific compliance programs and is continually assessed by external certifying bodies and independent auditors to provide assurance the policies, processes, and controls established and operated by AWS are in alignment with these program standards and the highest open standards.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 4.3 Security Standards - IV. Cyber Hygiene Practices | AWS            | <p>AWS Control Objective:</p> <p>Governance and Risk Management - Shared Responsibility Model</p> | <p>Security and compliance is a shared responsibility between AWS and the customer. AWS is responsible for the security and compliance 'of' the cloud, and implements security controls to secure the underlying infrastructure that runs the AWS services and hosts and connects customer resources. AWS customers are responsible for security 'in' the cloud and should determine, design and implement the security controls needed based on their security and compliance needs and AWS services they select. The customer responsibility will be determined by the AWS services that a customer selects. AWS provides customers with best practices on how to secure their resources within the AWS service's documentation at <a href="http://docs.aws.amazon.com/">http://docs.aws.amazon.com/</a>.</p> <p>AWS customers are responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Refer to <a href="http://aws.amazon.com/security/penetration-testing">http://aws.amazon.com/security/penetration-testing</a> for terms of service regarding penetration testing. Penetration tests should include customer IP addresses and not AWS endpoints.</p> |

| Requirement | Responsibility | AWS supporting information | Additional information                                                  |
|-------------|----------------|----------------------------|-------------------------------------------------------------------------|
|             |                |                            | AWS endpoints are tested as part of AWS compliance vulnerability scans. |

Table 5 — Guidance provided by the AWS Well-Architected Framework to the Cyber Hygiene Practice 4.3

| Requirement                                          | Responsibility | AWS Supporting information                                                                                                                                         | Additional information                                                                                                              | Learn more                 |
|------------------------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| 4.3 Security Standards - IV. Cyber Hygiene Practices | Customer       | Well-Architected - Question/ Best Practice:<br><br>OPS-3 - How do you reduce defects, ease remediation, and improve flow into production? - Share design standards | Share best practices across teams to increase awareness and maximize the benefits of development efforts.                           | <a href="#">Learn more</a> |
| 4.3 Security Standards - IV. Cyber Hygiene Practices | Customer       | Well-Architected - Question/ Best Practice:<br><br>SEC-7 - How do you protect your compute resources? - Automate configuration management                          | Enforce and validate secure configurations automatically by using a configuration management service or tool to reduce human error. | <a href="#">Learn more</a> |
| 4.3 Security Standards - IV. Cyber Hygiene Practices | Customer       | Well-Architected - Question/ Best Practice:<br><br>SEC-6 - How do you protect your networks? - Automate configuration management                                   | Enforce and validate secure configurations automatically by using a configuration management service or tool to reduce human error. | <a href="#">Learn more</a> |

FIs can create an AWS account at [AWS Artifact](#) and get a copy of the AWS Workbook for MAS Notice 655 on Cyber Hygiene from the [AWS Artifact portal](#) after logging in.

FIs should review responses from AWS in the AWS Workbook for MAS Notice 655 on Cyber Hygiene, and enrich them with the FI’s own company-wide controls.

# ABS Cloud Computing Implementation Guide 2.0

The Association of Banks in Singapore (ABS) has also published an implementation guide for banks that are entering into cloud outsourcing arrangements. The *ABS Cloud Computing Implementation Guide 2.0* includes recommendations that were discussed and agreed by members of the ABS Standing Committee for Cyber Security, and are intended to assist banks in further understanding approaches to due diligence, vendor management, and key controls that should be implemented in cloud outsourcing arrangements. Importantly, while the *MAS Guidelines on Outsourcing and Technology Risk Management Guidelines* are issued by the relevant regulator and provide guidance for a broad class of financial institutions, the *ABS Cloud Computing Implementation Guide 2.0* comprises a series of practical recommendations from the banking industry body.

## Key controls

The *ABS Cloud Computing Implementation Guide* recommends that a number of key controls be implemented when entering into a cloud outsourcing arrangement.

AWS has produced the AWS Workbook for ABS Cloud Computing Implementation Guide 2.0 that maps AWS security and compliance controls (*OF the cloud*) and best practice guidance provided by the [AWS Well-Architected Framework](#) (*IN the cloud*) to the requirements within the guide. Where applicable, under the AWS Shared Responsibility Model, the workbook provides supporting details and references to assist FIs when they adapt the guide for their workloads on AWS.

The following table excerpt shows an example of the response from AWS to controls in *section 4 - C) Run the Cloud - 1. Change Management – Considerations/Standard Workloads* of the [ABS Cloud Computing Implementation Guide 2.0](#):

Table 6 — Response from AWS to controls in section 4.C.1

| Requirement                                                                                                                                                                                                                                                      | Responsibility | AWS supporting information                                                                          | Additional information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Learn more |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <p>1. Change management procedures should be mutually agreed between the CSP and the FI. Such procedures should be formalized, and include change request and approval procedures, as well as a reporting component. - Considerations for Standard Workloads</p> | <p>AWS</p>     | <p>AWS Control Objective:<br/><br/>Governance and Risk Management - Shared Responsibility Model</p> | <p>Security and compliance is a shared responsibility between AWS and the customer. AWS is responsible for the security and compliance 'of' the cloud, and implements security controls to secure the underlying infrastructure that runs the AWS services and hosts and connects customer resources. AWS customers are responsible for security 'in' the cloud and should determine, design and implement the security controls needed based on their security and compliance needs and AWS services they select. The customer responsibility will be determined by the AWS services that a customer selects.</p> <p>AWS provides customers with best practices on how to secure their resources within the AWS service's documentation at <a href="http://docs.aws.amazon.com/">http://docs.aws.amazon.com/</a>.</p> <p>AWS customers are responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Refer to <a href="http://aws.amazon.com/security/penetration-testing">http://aws.amazon.com/security/penetration-testing</a> for terms of service regarding penetration testing. Penetration tests should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans.</p> | <p>n/a</p> |

| Requirement                                                                                                                                                                                                                                                      | Responsibility | AWS supporting information                   | Additional information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Learn more  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| <p>1. Change management procedures should be mutually agreed between the CSP and the FI. Such procedures should be formalized, and include change request and approval procedures, as well as a reporting component. - Considerations for Standard Workloads</p> | <p>AWS</p>     | <p>AWS Control Objective:<br/><br/>OSPAR</p> | <p>The Association of Banks in Singapore (ABS) Guidelines on Control Objectives and Procedures for Outsourced Service Providers (ABS Guidelines) recommend that Singapore banks select outsourced service providers that meet the controls set out in the ABS Guidelines, which can be demonstrated through an OSPAR. Amazon Web Services (AWS) achieved the Outsourced Service Provider’s Audit Report (OSPAR) attestation.</p> <p>An OSPAR attestation involves an external audit of the service provider’s controls against the criteria specified in the ABS Guidelines. The audit report can be downloaded on AWS Artifact.</p> | <p>n/ a</p> |

| Requirement                                                                                                                                                                                                                                               | Responsibility | AWS supporting information                                                                                                   | Additional information                                | Learn more                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|----------------------------|
| 1. Change management procedures should be mutually agreed between the CSP and the FI. Such procedures should be formalized, and include change request and approval procedures, as well as a reporting component. - Considerations for Standard Workloads | Customer       | Well-Architected - Question/ Best Practice:<br><br>REL-5 - How do you implement change? - Deploy changes in a planned manner | Deployments and patching follow a documented process. | <a href="#">Learn more</a> |

FIs can create an AWS account at [AWS Artifact](#) and get a copy of the AWS Workbook for ABS Cloud Computing Implementation Guide 2.0 from the [AWS Artifact portal](#) after logging in.

FIs should review responses from the AWS Workbook for ABS Cloud Computing Implementation Guide 2.0, and enrich them with the FI's own company-wide controls.

## Next steps

Each organization's cloud adoption journey is unique. To successfully complete cloud adoption, FIs need to understand their organization's current state, the target state, and the transition required to achieve the target state. Knowing this will help FIs set goals and create work streams that will enable a successful move to the cloud.

The [AWS Cloud Adoption Framework](#) (AWS CAF) offers structure to help organizations develop an efficient and effective plan for their cloud adoption journey. Guidance and best practices prescribed in the Framework can help FIs build a comprehensive

approach to cloud computing across their organization, throughout their IT lifecycle. The [AWS CAF](#) breaks down the complicated process of planning into manageable areas of focus.

Many organizations choose to apply the AWS CAF methodology with a facilitator-led workshop. To find more about such workshops, contact your AWS representative. Alternatively, AWS provides access to tools and resources for self-service application of the AWS CAF methodology at [AWS Cloud Adoption Framework](#).

For FIs regulated by the Monetary Authority of Singapore (MAS), next steps typically also include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, as well as AWS solution architects, Professional Services teams, and training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, [contact AWS](#).
- Obtain and review a copy of the latest AWS SOC 1 and 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification, from the [AWS Artifact](#) portal (accessible via the AWS Management Console).
- Consider the relevance and application of the [CIS Amazon Web Services Foundations](#), as appropriate for your cloud journey and use cases. These industry-accepted best practices published by the Center for Internet Security go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.
- Dive deeper on other governance and risk management practices as necessary in light of your due diligence and risk assessment, using the tools and resources referenced throughout this whitepaper and in the Additional Resources section below.
- Speak with your AWS representative to learn more about how AWS is helping financial services customers migrate their critical workloads to the cloud.
- Review a copy of the AWS MAS TRM Workbook, Notice 655 on Cyber Hygiene Workbook and ABS Cloud Computing Implementation Guide 2.0 Workbook from the AWS Artifact portal (accessible through the AWS Management Console). FIs should populate the workbook with additional controls that they have implemented or will implement.

- Update and maintain your register of outsourcing arrangements as appropriate, for submission to MAS at least annually or upon request.

## Conclusion

Providing highly secure and resilient infrastructure and services to customers is a top priority for AWS. The AWS commitment to customers is focused on working to continuously earn customer trust and ensure customers maintain confidence in operating their workloads securely on AWS. To achieve this, AWS has integrated risk and compliance mechanisms that include:

- The implementation of a wide array of security controls and automated tools
- Nearly continuous monitoring and assessment of security controls to help ensure AWS operational effectiveness and strict adherence to compliance regimes

In addition, AWS regularly undergoes independent third-party audits to provide assurance that the control activities are operating as intended. These audits, along with the many certifications AWS has obtained, provide an additional level of validation of the AWS control environment that benefits customers.

Taken together with customer managed security controls, these efforts allow AWS to securely innovate on behalf of customers and help customers improve their security posture when building on AWS.

## Additional resources

Set out below are additional resources to help financial institutions think about security, compliance and designing a secure and resilient AWS environment.

- [AWS Compliance Quick Reference Guide](#) — AWS has many compliance-enabling features that you can use for your regulated workloads in the AWS Cloud. These features can allow you to achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry, easier operations, and improved agility by providing more oversight, security control, and central automation.

- **[AWS Well-Architected Framework](#)** — The Well-Architected Framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help implement designs that will scale application needs over time. The Well-Architected Framework consists of five pillars: Operational Excellence; Security; Reliability; Performance Efficiency; Cost Optimization.
- **Global Financial Services Regulatory Principles** — AWS has identified five common principles related to financial services regulation that customers should consider when using AWS Cloud services and specifically, when applying the shared responsibility model to their regulatory requirements. Customers can access a whitepaper on these principles under a nondisclosure agreement at [AWS Artifact](#).
- **NIST Cybersecurity Framework (CSF)** — The AWS whitepaper [NIST Cybersecurity Framework \(CSF\): Aligning to the NIST CSF in the AWS Cloud](#) demonstrates how public and commercial sector organizations can assess the AWS environment against the NIST CSF and improve the security measures they implement and operate (security **in** the cloud). The whitepaper also provides a third-party auditor letter attesting to the AWS Cloud offering's conformance to NIST CSF risk management practices (security **of** the cloud). FIs can leverage NIST CSF and AWS resources to elevate their risk management frameworks.
- **[Using AWS in the Context of Common Privacy and Data Protection Considerations](#)** — This document provides information to assist customers who want to use AWS to store or process content containing personal data, in the context of common privacy and data protection considerations. It will help customers understand:
  - The way AWS services operate, including how customers can address security and encrypt their content.
  - The geographic locations where customers can choose to store content; and, other relevant considerations.
  - The respective roles the customer and AWS each play in managing and securing content stored on AWS services.

## Contributors

Contributors to this document include:

- Bella Khabbaz, Senior Corporate Counsel, Amazon Web Services
- Alvin Li, Sr Security Strategist, Amazon Web Services
- Brandon Lim, Principal FS Security, Amazon Web Services
- Daniel Wu, Principal Public Policy, Amazon Web Services
- Genevieve Ding, Public Policy Head SG & ASEAN, Amazon Web Services
- Melissa Yoong, Public Policy Manager SG, Amazon Web Services

## Document revisions

| Date                   | Description                                                                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>January 3, 2022</b> | Third publication. Updated MAS TRMG, ABS Cloud Computing Implementation Guidelines 2.0 to reflect the updated AWS TRMG Workbook and new ABS Cloud Computing Implementation Guide 2.0. |
| <b>May 2019</b>        | Second publication. Updated MAS TRM section to reflect the security in the cloud guidance provided by AWS Well-Architected and the associated enhanced MAS TRM Guidance Workbook.     |
| <b>July 2017</b>       | First publication                                                                                                                                                                     |