

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

*May 2019*



## 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.

© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Contents

- Introduction ..... 1
- The Shared Responsibility Model .....2
- Security of the Cloud .....4
  - Assurance Programs.....5
  - AWS Artifact .....7
- AWS Regions .....7
- MAS Guidelines on Outsourcing.....8
  - Assessment of Service Providers .....8
  - Cloud Computing.....13
  - Outsourcing Agreements .....18
  - Audit and Inspection.....18
- MAS Technology Risk Management Guidelines .....19
- ABS Cloud Computing Implementation Guide .....25
  - Activities Recommended for Due Diligence .....25
  - Key Controls .....29
- Next Steps .....36
- Contributors .....37
- Additional Resources .....38
- Document Revisions.....39

# 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.

## Introduction

In July 2016, the Monetary Authority of Singapore (MAS) updated the *Guidelines on Outsourcing* for financial institutions (FIs) to acknowledge 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. While the use of AWS services by Singapore's FIs substantially predates the update to the *Guidelines on Outsourcing*, AWS welcomes the increased clarity and guidance provided by the MAS.

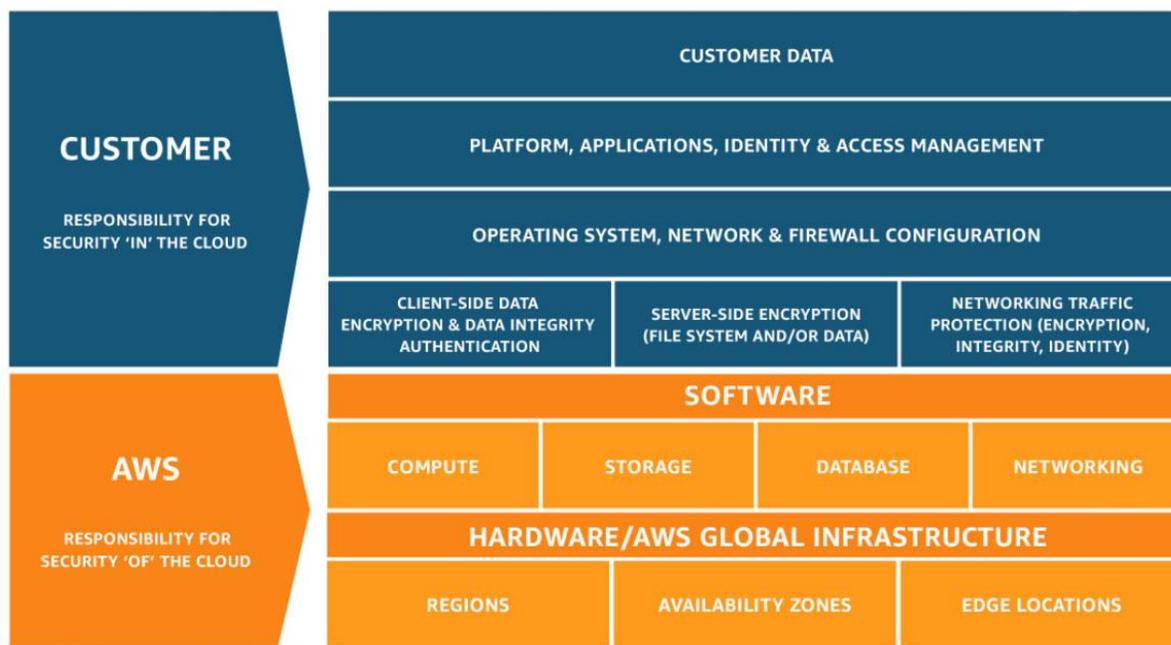
The following sections provide considerations for FIs as they assess their responsibilities related to the following guidelines:

- **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.
- **Association of Banks in Singapore (ABS) Cloud Computing Implementation Guide** – 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.

## The Shared Responsibility Model

Before exploring the requirements included in the various guidelines, it is important that FIs understand the AWS Shared Responsibility Model (*Figure 1*).



*Figure 1 – AWS Shared Security Responsibility Model*

This shared responsibility model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles.

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. Much like a traditional data center, the customer is responsible for managing the guest operating system (including installing updates and security patches) and 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 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 that controls are operating effectively in their extended IT environment. For more information, see 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, see [Using AWS in the Context of Singapore Privacy Considerations](#).

## Security of the Cloud

To provide Security of the Cloud, AWS environments are 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 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.

## Assurance 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, see <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, see <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, see <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, see <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, see <https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/>
- **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, see <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, see <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

By tying together governance-focused, audit-friendly service features with such certifications, attestations, and audit standards, AWS Compliance enablers build on traditional programs, and help customers to establish and operate in an AWS security control environment.

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

For a description of general security controls and service-specific security from AWS, see [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 current information on AWS Regions and Availability Zones, see <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 be able to 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 most frequently arise 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, including use of the cloud. The following table includes considerations for each component of 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 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 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 includes issues such as compliance with laws, conflicts of interest, bribery, discrimination and harassment, health and safety, recordkeeping, and financial integrity.</p> <p>The Amazon.com, Inc. Form 10-K filing is available at the Amazon Investor Relations website or the website of the US Securities and Exchange Commission, and includes details of legal proceedings involving Amazon.com, Inc., Amazon Web Services, Inc., and other affiliates.</p>

Due Diligence Requirement	AWS Response
5.4.3 (d) Security and internal controls, audit coverage, reporting and monitoring environment	<p>An AWS Chief Information Security Officer (CISO) exists and is responsible for coordinating, developing, implementing, and maintaining an organization-wide information security program.</p> <p>AWS management re-evaluates the security program at least biannually. This process requires management to identify risks within its areas of responsibility and to implement 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, see the AWS Compliance Center.</p> <p>Compliance reports from these assessments are made available through AWS Artifact 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. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.</p>
5.4.3 (e) Risk management framework and capabilities, including technology risk management and business continuity management in respect of the outsourcing arrangement	<p>AWS management has developed a strategic business plan, which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.</p>

Due Diligence Requirement	AWS Response
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 to ensure system availability in the event of component failure. 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 eliminate 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> <p>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.</p>

Due Diligence Requirement	AWS Response
5.4.3 (g) Reliance on and success in dealing with subcontractors	<p>AWS uses a number of third-party subcontractors to assist with the provision of its service.</p> <p>However, our subcontractors do not have access to customers' content. In addition, AWS only uses subcontractors that we trust and we use appropriate contractual safeguards which we monitor to ensure the required standards are maintained.</p>
5.4.3 (h) Insurance coverage	<p>AWS maintains appropriate insurance, including Commercial General Liability insurance with limits of not less than \$1,000,000 per occurrence and \$5,000,000 general aggregate, and (b) <i>Crime/Employee Dishonesty</i> insurance with limits of not less than \$500,000 per claim.</p>
<p>5.4.3 (i) External environment (such as the political, economic, social and legal environment of the jurisdiction in which the service provider operates);</p> <p>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.</p>	<p>AWS works to comply with applicable federal, state, and local laws, statutes, ordinances, and regulations concerning security, privacy and data protection of AWS services in order to minimize the risk of accidental or unauthorized access or disclosure of customer content.</p> <p>AWS formally tracks and monitors its regulatory and contractual agreements and obligations. In order to do so, AWS has performed and maintains the following activities:</p> <ol style="list-style-type: none"> <li>1. Identified applicable laws and regulations for each of the jurisdictions in which AWS operates.</li> <li>2. Documented and maintains all statutory, regulatory, and contractual requirements relevant to AWS.</li> </ol>

## 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 that 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 preliminary responses that are relevant to each risk mentioned in paragraph 6.7 of the *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 have 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, and where it is stored, used, and protected from disclosure.</p> <p>Customer-provided data is validated for integrity, and corrupted or tampered data is not written to storage. 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>

Risk Area	AWS Controls
Sovereignty	<p>AWS customers control 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. For more information, see <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, uninterruptable 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 data-bbox="581 275 1333 380">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 data-bbox="630 401 1438 915" style="list-style-type: none"><li data-bbox="630 401 1341 474">• Identified applicable laws and regulations for each of the jurisdictions in which AWS operates</li><li data-bbox="630 485 1341 558">• Documented and maintains all statutory, regulatory, and contractual requirements relevant to AWS</li><li data-bbox="630 569 1438 653">• Categorized records into types with details of retention periods and type of storage media through the Data Classification Policy</li><li data-bbox="630 663 1422 831">• 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 data-bbox="630 842 1438 915">• Monitors the use of AWS facilities for unauthorized activities with a process in place to enforce appropriate disciplinary action</li></ul> <p data-bbox="581 926 1422 1073">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 data-bbox="581 1083 1382 1157">For more information, see the following AWS Audit Reports: SOC 1, SOC 2, PCI DSS, ISO 27001, ISO 27017</p>

Risk Area	AWS Controls
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> <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. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.</p> <p>Some of our key audit programs and certifications are described in the <a href="#">Assurance Programs</a> section. For a full list of audits, certifications, and attestations, see the <a href="#">AWS Compliance Center</a>.</p>
Segregation of customer data	<p>The deployment model is a virtual private cloud implemented with the Amazon Virtual Private Cloud service from AWS.</p> <p>Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.</p> <p>Details of customer isolation and data segregation can be found in the AWS SOC2 report.</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, see [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, but include an important clarification that such audits may be carried out by the service provider's external auditors.

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, see the [AWS Well-Architected homepage](#).

The following table excerpt shows an example of the response from AWS to guideline 11.1 in the TRM Guidelines:

Requirement	Responsibility	Source	Section	AWS Supporting Information	Additional Information
11. Access Control – 11.1 User Access Management	AWS	AWS Control Objectives	AWS Control Section: Governance and Risk Management	AWS Control Objective: Governance and Risk Management – Shared Responsibility Model	<p><i>Security and compliance</i> 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 <i>in</i> the cloud and should determine, design, and implement security controls based on their security and compliance needs and the AWS services they select. The customer responsibility is determined by the AWS services that a customer selects. AWS provides customers with best practices on how to secure their resources in the AWS service 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. For the terms of service regarding penetration testing, see <a href="#">Penetration Testing</a> on the AWS website. Penetration tests should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans.</p>

Requirement	Responsibility	Source	Section	AWS Supporting Information	Additional Information
11. Access Control – 11.1 User Access Management	AWS	AWS Control Objectives	AWS Control Section: Identity & Access Management	AWS Control Objective: Identity & Access Management – User Access Management	<p>For more information, see the following AWS Audit Reports: MTCS, HKMA TM-G-1, PCI 3.2, ISO 27001, ISO 27017, HIPAA, IRAP, NIST 800-53 (FEDRAMP &amp; DOD), SOC 2 COMMON CRITERIA, SOC 1 &amp; 2 CONTROLS, K-ISMS, C5</p> <p>User access to the internal Amazon network is not provisioned unless an active record is created in the HR System by Human Resources. Access is automatically provisioned with least privilege per job function. First time passwords are set to a unique value and changed immediately after first use.</p> <p>IT access above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.</p> <p>IT access privileges are reviewed on a quarterly basis by appropriate personnel.</p> <p>For more information, see the following AWS Audit Reports: HKMA TM-G-1, PCI 3.2, ISO 27001, ISO 27017, ISO 27018, NIST 800-53 (FEDRAMP &amp; DOD), SOC 2 COMMON CRITERIA, K-ISMS, C5</p>

Requirement	Responsibility	Source	Section	AWS Supporting Information	Additional Information
11. Access Control – 11.1 User Access Management	AWS	AWS Control Objectives	AWS Control Section: Identity & Access Management	AWS Control Objective: Identity & Access Management – User Access Revocation	User access rights to AWS systems (for example, network, applications and tools) is revoked within 24 hours of termination or deactivation. Inactive user accounts are disabled and removed at least every 90 days.  For more information, see the following AWS Audit Reports: HKMA TM-G-1, PCI 3.2, ISO 27001, ISO 27017, ISO 27018, HIPAA, NIST 800-53 (FEDRAMP & DOD), SOC 1 & 2 CONTROLS, K-ISMS, C5

Requirement	Responsibility	Source	Section	AWS Supporting Information	Additional Information	Learn More
11. Access Control – 11.1 User Access Management	Customer	Well-Architected	Security Pillar	Well-Architected – Question/Best Practice: SEC-1 – How do you manage credentials and authentication? – Define identity and access management requirements	Identity and access management configurations need to be defined to meet your organizational, legal, and compliance requirements.	<a href="#">Learn More...</a>
11. Access Control – 11.1 User Access Management	Customer	Well-Architected	Security Pillar	Well-Architected – Question/Best Practice: SEC-1 – How do you manage credentials and authentication? – Secure AWS root user	Secure the AWS root user with MFA, no access keys, and limit its use to help secure your AWS account.	<a href="#">Learn More...</a>

Requirement	Responsibility	Source	Section	AWS Supporting Information	Additional Information	Learn More
11. Access Control – 11.1 User Access Management	Customer	Well-Architected	Security Pillar	Well-Architected – Question/Best Practice: SEC-1 – How do you manage credentials and authentication? – Enforce use of multi-factor authentication	Enforce multi-factor authentication (MFA) with software or hardware mechanisms to provide additional access control.	<a href="#">Learn</a> <a href="#">More...</a>

FIs can get a copy of the AWS MAS TRM Workbook from the [AWS Artifact](#) portal.

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.

# ABS Cloud Computing Implementation Guide

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* 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* comprises a series of practical recommendations from the banking industry body.

The following sections include information about due diligence and controls recommended by ABS, and address key concepts from Section 3 and 4 of the *ABS Cloud Computing Implementation Guide*.

## Activities Recommended for Due Diligence

### 1. Contractual Considerations

The *ABS Cloud Computing Implementation Guide* includes a series of recommendations for contracts with a cloud service provider (CSP), including that the FI should ensure that it has the ability to contractually enforce agreed and measurable information security and operational requirements.

AWS customers have the option to enroll in an Enterprise Agreement with AWS. For more information about AWS Enterprise Agreements, contact your AWS representative.

### 2. Data Center

In summary, the *ABS Cloud Computing Implementation Guide* recommends proper due diligence be conducted on a cloud provider's data center and that, where it is not possible to perform onsite due diligence, an independent assessment report (such as SOC 2 / ISO 27001 / ISO 27018) should be provided by the cloud service provider for all the data centers that process and store the FI's data.

To learn more about data centers, see these resources:

- [AWS Risk and Compliance](#) whitepaper
- [AWS Data Centers](#) on the AWS website
- [Overview of Security Processes](#) whitepaper
- AWS SOC 2 Report available in AWS Artifact
- ISO 27001 and ISO 27108 certifications available in AWS Artifact

The [AWS Singapore Multi-Tier Cloud Security Standard \(MTCS SS 584\)](#) Level-3 (CSP) certification also provides additional assurance to customers that they can host and process their highly confidential data in Singapore on AWS.

### 3. Data Sovereignty

The *ABS Cloud Computing Implementation Guide* recommends that FIs consider the social, political and economic climate of a country before an FI places its data there.

AWS customers designate in which physical region their data and their servers will be located. For current information on AWS Regions and Availability Zones, see <https://aws.amazon.com/about-aws/global-infrastructure/>. The AWS Singapore region, which customers can select as their primary region, provides multiple Availability Zones for resiliency. AWS will not move customer data outside of the customer's chosen regions, except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users.

### 4. Data Retention

The *ABS Cloud Computing Implementation Guide* recommends that an FI controls access to its data, whether used for operational purposes or for contingency, disaster recovery and backups.

AWS provides an advanced set of access, encryption, and logging features to help customers manage the security of their content, as well as AWS services for data retention.

In particular, AWS provides multiple options for backup and encryption of customer data. Customers can use Amazon S3 or Amazon Glacier for storage of backup data. All Amazon S3 and Amazon Glacier API endpoints support SSL encryption for data in transit. Amazon Glacier encrypts all data at rest by default. With Amazon S3, customers can choose server-side encryption for objects at rest by letting AWS manage the encryption keys, providing their own keys when they upload an object, or using AWS Key Management Service (AWS KMS) integration for the encryption keys. Alternatively, customers can always encrypt their data before uploading it to AWS.

For more information about data storage, see the [Overview of AWS Security - Storage Services](#) paper.

For more information about encryption, see these papers:

- [AWS Key Management Service Cryptographic Details](#)
- [Encrypting Data at Rest](#)

## 5. Governance

The *ABS Cloud Computing Implementation Guide* recommends that cloud service providers be able to demonstrate that internal governance mechanisms exist to ensure regular review of its risk profile and risk management decisions.

AWS management has developed a strategic business plan that includes risk identification and the implementation of controls to mitigate or manage risks. AWS management reevaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.

For more information, see the [AWS Risk and Compliance](#) paper. For assurances, you can get a copy of the most recent AWS SOC 2 Report, as well as the ISO 27001 and ISO 27108 certifications.

## 6. Exit Plan

The *ABS Cloud Computing Implementation Guide* recommends that FIs have an appropriate exit plan that is appropriate for the materiality of the outsourcing. FIs should consider transferability of outsourced services to another third party or back to the FIs data centers for continuity of service.

Customers manage access to their customer content and AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Snowball to transfer large amounts of data into and out of AWS using physical storage appliances. For more information, see <https://aws.amazon.com/products/storage/>.

Additionally, AWS offers AWS Database Migration Service, a web service that customers can use to migrate a database from an AWS service to an on-premises database.

The *ABS Cloud Computing Implementation Guide* also recommends that FIs should consider the use of procedures and tools to ensure deletion of data in a manner where data is rendered irrecoverable.

AWS provides customers with the ability to delete their data. Because AWS customers retain control and ownership of their data, it is the customer's responsibility to manage data retention to their own requirements.

In alignment with ISO 27001 standards, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (*National Industrial Security Program Operating Manual*) or NIST 800-88 (*Guidelines for Media Sanitization*) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. For more information, see ISO 27001 standards: Annex A, domain 8. AWS has been validated and certified by an independent auditor to confirm alignment with the ISO 27001 certification standard.

## 7. Financial and Continuity Risk

The *ABS Cloud Computing Implementation Guide* recommends that the FI periodically review the financial and operational capabilities of the cloud service provider.

AWS is a leading cloud provider and is a long-term business strategy of Amazon.com. AWS has very high, long term, sustainability potential. The financial statements of Amazon.com, Inc. include AWS sales and income, permitting assessment of its financial position and ability to service its debts and liabilities. These financial statements are available from the SEC or at the Amazon Investor Relations website.

## Key Controls

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

The following table addresses considerations for use of AWS in relation to the 12 key controls documented within the *ABS Cloud Computing Implementation Guide*:

Key Control	Guideline	AWS Considerations	Service Considerations
<b>Encryption</b>	FIs are encouraged to develop a comprehensive data loss prevention strategy to protect confidential information stored on endpoints, in motion, and at rest.	Customers choose how their customer content is secured. AWS offers customers strong encryption for customer content in transit or at rest, and provides customers with the option to manage their own encryption keys.	AWS Key Management Service (KMS) AWS CloudHSM
<b>Tokenization</b>	It is in the best interest of the FI to minimize its data footprint to reduce the vulnerability surface and potential threat vectors.	Where tokenization of data is desired before leaving your organization this can be achieved through a number of AWS partners with offerings available in the marketplace.	AWS Marketplace

Key Control	Guideline	AWS Considerations	Service Considerations
<b>Dedicated Equipment &amp; Private Cloud</b>	FIs are recommended to risk assess the logical segregation controls present within the virtual environment. FIs can leverage the AWS Security Assurance programs detailed previously in this document (such as the SOC2 report) to gain an understanding of controls implemented by AWS.	Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.	Amazon Virtual Private Cloud (Amazon VPC) AWS Direct Connect VPN
<b>Change Management &amp; Privileged User Access Management (PUAM)</b>	The ABS guidelines state that FIs are expected to maintain effective control over their data, with consideration given to the application, OS, database, and network layers. FIs are also expected to manage change within their environment appropriately.	Customers retain the ability to manage segregations of duties of their AWS resources, as well as to monitor the changes made to the environment through AWS Config and AWS CloudTrail.	AWS Identity Access Management (IAM) AWS CloudTrail AWS Config

Key Control	Guideline	AWS Considerations	Service Considerations
<b>Virtualized Environment Security</b>	The ABS guidelines recommend that consideration is given to the risks associated with virtualization software, such as hypervisors and the operating system images used by the FI.	Virtual instances are completely controlled by the customer. Customers have full root access or administrative control over accounts, services, and applications.  AWS does not have any access rights to customer instances or the guest OS. AWS recommends a base set of security best practices to include disabling password-only access to your guests, and using some form of multi-factor authentication to gain access to customer instances (at a minimum, certificate-based SSH Version 2 access)	Amazon Virtual Private Cloud (Amazon VPC)  PCI-DSS Compliance

Key Control	Guideline	AWS Considerations	Service Considerations
<b>User Access Management &amp; Segregation of Duties</b>	The ABS guidelines recommend that FIs consider the full life-cycle of user access when implementing a cloud outsourcing arrangement.	AWS provides a number of ways for customers to identify users and securely access their AWS account. A complete list of credentials supported by AWS can be found on the Security Credentials page under <b>Your Account</b> . AWS also provides additional security options that enable customers to further protect their AWS account and control access: AWS Identity and Access Management (AWS IAM), key management and rotation, temporary security credentials, and multi-factor authentication (MFA).	AWS Identity Access Management (IAM) AWS Multi-Factor Authentication (MFA)

Key Control	Guideline	AWS Considerations	Service Considerations
<b>Collaborative Disaster Recovery Testing</b>	The ABS guidelines state that disaster recovery testing is an essential part of developing an effective disaster recovery strategy. FIs are recommended to plan and perform their own simulated disaster recovery testing.	<p>The ABS guidelines state that cloud service providers should obtain necessary certifications such as ISO27001 and ISO27018.</p> <p>The AWS implementation of and alignment with ISO 27001, 27017, and 27018 demonstrates a commitment to information security at every level of the organization.</p> <p>AWS provides customers with the capability to implement a robust continuity plan, including using 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. For more information about approaches to disaster recovery, see <a href="https://aws.amazon.com/disaster-recovery/">https://aws.amazon.com/disaster-recovery/</a>.</p>	<p>Global Infrastructure (Regions, Availability Zones)</p> <p>AWS Route 53</p> <p>AWS Elastic Load Balancing (ELB)</p>

Key Control	Guideline	AWS Considerations	Service Considerations
<b>Security Events Monitoring &amp; Incident Management</b>	ABS states that the compromise of a system can only be detected in a timely fashion if there is effective monitoring in place to detect abnormal activities. As part of the shared security responsibility model, security events monitoring should be performed by both AWS and the financial institution.	AWS has implemented a formal, documented incident response policy and program, which can be reviewed in the SOC 2. Customers can also see all security notifications through AWS Service Health Dashboard or the AWS Personal Health Dashboard. AWS customers can use various tools to monitor for abnormalities, including those mentioned here and from AWS Marketplace.	AWS CloudTrail, Amazon CloudWatch VPC Flow Logs Amazon Elasticsearch Service
<b>Penetration Testing &amp; Vulnerability Management</b>	The ABS guidelines state that testing the security of applications and infrastructure provides assurance of the security posture of a service. FIs are recommended to perform vulnerability assessment and penetration at regular frequency.	Customers can request permission to conduct scans of their cloud infrastructure, if they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request through the AWS Vulnerability / Penetration Testing Request Form at <a href="https://aws.amazon.com/forms/penetration-testing-request">https://aws.amazon.com/forms/penetration-testing-request</a> .	AWS Trusted Advisor Third-party products from AWS Marketplace

Key Control	Guideline	AWS Considerations	Service Considerations
<b>Administrative Remote Access</b>	The ABS guidelines recommend that FIs consider the risks associated with remote access and that strict controls be implemented.	Virtual instances are solely controlled by the customer. AWS personnel do not have the ability to log in to customer instances.  Customers have full root access or administrative control over accounts, services, and applications. Customers can also disable password-only access to guests, and use some form of multi-factor authentication to gain access to customer instances (at a minimum key-based SSH Version 2 access).	AWS Identity Access Management (IAM) AWS Multi-Factor Authentication (MFA) Third party products from AWS Marketplace
<b>Secure Software Development Lifecycle &amp; Code Reviews</b>	The ABS guidelines recommend that risk assessment, threat modelling, vulnerability assessment, security testing, configuration review, remediation, and security improvement processes are adopted for cloud applications.	The AWS development process follows secure software development best practices, which include formal design reviews by the AWS Security Team, threat modeling, and completion of a risk assessment. For more information, see the AWS SOC 2.	AWS CodeCommit AWS CodePipeline

Key Control	Guideline	AWS Considerations	Service Considerations
<b>Securing Logs &amp; Backups</b>	ABS recommends that FIs develop a backup strategy for storing critical information. The backup strategy should be periodically tested and validated to make sure that the backup media can sufficiently support the FIs recovery process.	Amazon S3 and Amazon Glacier are ideal services for backup and archiving. Both are durable, low-cost storage platforms. Both offer unlimited capacity and require no volume or media management as backup data sets grow.	Amazon S3 Amazon Glacier AWS Storage Gateway AWS Key Management Service (KMS)

## Next Steps

Each organization's cloud adoption journey is unique. To successfully execute 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. For more information about these workshops, contact your AWS representative. AWS also provides access to tools and resources for self-service application of the AWS CAF methodology at <https://aws.amazon.com/professional-services/CAF/>

For FIs in Singapore, next steps typically also include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, AWS Solution Architects team, AWS Professional Services team, and AWS Training instructors, can help with your cloud adoption journey. If you don't have an AWS representative, contact AWS at <https://aws.amazon.com/contact-us/>.
- Review a copy of the latest AWS Service Organization Control 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification, from the AWS Artifact portal (accessible through the AWS Management Console).
- Review a copy of the AWS MAS TRM 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.
- Consider the relevance and application of the [CIS AWS Foundations Benchmark](#) paper, as appropriate for your cloud journey and use cases. These industry-accepted best practices published by the Center for Internet Security (CIS) go beyond the high-level security guidance already available, and provide AWS users with clear, step-by-step implementation and assessment recommendations.
- Dive deeper on other governance and risk management practices as necessary based on what you discover during your due diligence and risk assessment phases, using the tools and resources referenced throughout this paper and in the [Additional Resources](#) section.
- Speak to your AWS representative about an AWS Enterprise Agreement, and the introductory guide designed to help Singapore's FIs assess the AWS Enterprise Agreement against the MAS *Guidelines on Outsourcing*.
- Update and maintain your register of outsourcing arrangements as appropriate, for submission to MAS at least annually or upon request.

## Contributors

Contributors to this document include:

- Darran Boyd, Principle Security Solutions Architect, Financial Services, APAC
- Myles Hosford, Principle Security Solutions Architect, ASEAN

## Additional Resources

For additional information, see the following papers, which can also be found on the [AWS Compliance Resources](#) page and the [AWS Cloud Security Resources](#) page:

- [AWS Well-Architected Framework](#)
- [AWS Best Practices for DDoS Resiliency](#)
- [AWS Security Checklist](#)
- [Cloud Adoption Framework - Security Perspective](#)
- [Introduction to AWS Security Processes](#)
- [Overview of AWS Security - Storage Services](#)
- [Overview of AWS Security - Database Services](#)
- [Overview of AWS Security - Compute Services](#)
- [Overview of AWS Security - Application Services](#)
- [Overview of AWS Security - Analytics, Mobile and Application Services](#)
- [Overview of AWS Security - Network Services](#)
- [AWS Security Best Practices](#)
- [Securing Data at Rest with Encryption](#)
- [AWS Risk & Compliance](#)
- [Using AWS in the Context of Singapore Privacy Considerations](#)
- [Security at Scale: Logging in AWS](#)
- [Security at Scale: Governance in AWS](#)
- [Secure Content Delivery with CloudFront](#)

## Document Revisions

Date	Description
<b>May 2019</b>	Second publication. Updated MAS TRM section to reflect the in the Cloud guidance provided by AWS Well-Architected and the associated enhanced MAS TRM Guidance Workbook.
<b>July 2017</b>	First publication