AWS User Guide to Financial Services Regulations in the Philippines

December 22, 2023

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. The information in this document is current as of the date of publication.

Contents

About this guide

This guide provides information to assist financial services institutions regulated by the Bangko Sentral Ng Pilipinas (BSFIs), as they adopt and accelerate their use of Amazon Web Services (AWS) cloud services.

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.
- Provides additional resources that BSFIs can use to help design and architect their AWS environment to be secure and meet regulatory expectations.

This guide also provides considerations for BSFIs as they assess their responsibilities under the following Bangko Sentral Ng Pilipinas (BSP) regulations when they use AWS cloud services:

- The Manual of Regulations for Banks (MORB) – (2020 Edition) Section 112, Appendix 78, and Appendix 103.
- Manual of Regulations for Non-Bank Financial Institutions (MORNBFI) – (2020 Edition) Section 112-T and Appendix Q-36.

Taken together, BSFIs can use this information to assist 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 AWS Shared Responsibility Model

Cloud security is a shared responsibility. Amazon Web Services (AWS) manages security of the cloud by ensuring that AWS infrastructure complies with global and regional regulatory requirements and best practices, but security in the cloud is the responsibility of the customer. What this means is that customers retain control of the security program they choose to implement to protect their own content, applications, systems, and networks, no differently than they would for applications in an on-premises data center.

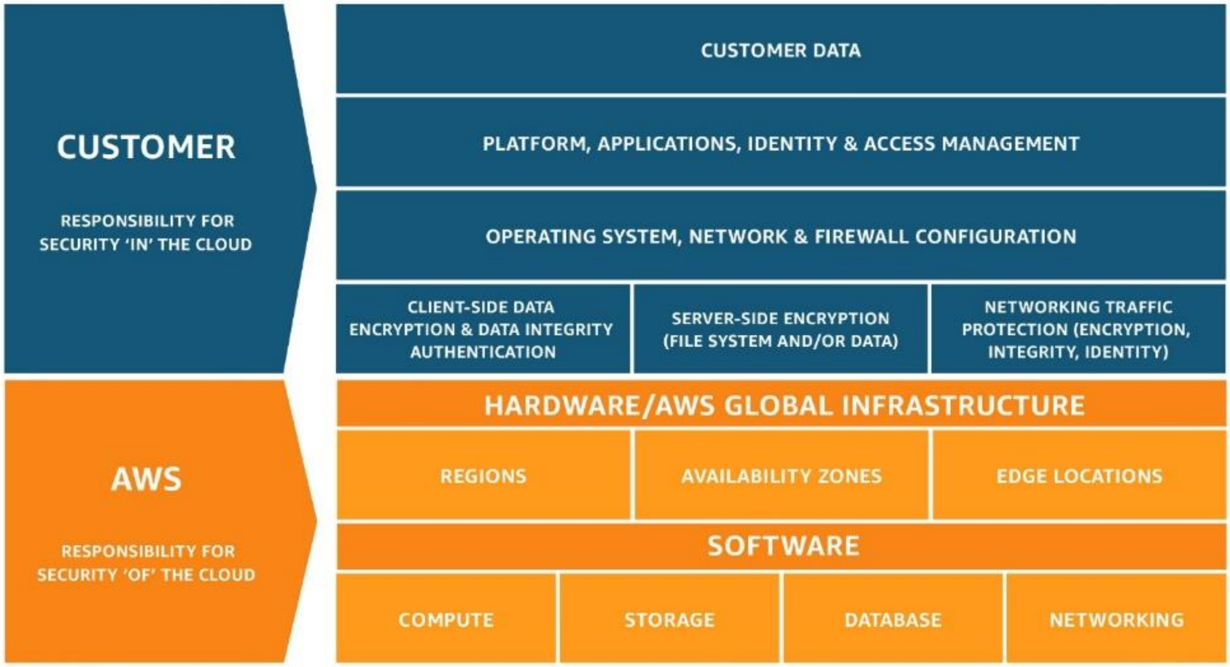
CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING

Figure 1: AWS Shared Responsibility Model

The Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of cloud security principles. AWS operates, manages, and controls the information technology (IT) components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve content. Customers are responsible for managing their content (including encryption options), classifying their assets, and using AWS Identity and Access Management (IAM) tools to apply the appropriate permissions.

Security in the cloud

Customers are responsible for their security in the cloud. 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 any applicable network security controls. Customers should carefully consider the services they choose, because their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations.

It’s important to note that when using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

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

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customer responsibility is determined by the AWS services that a customer selects. This selection, in turn, determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

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 Philippines Privacy Considerations.

Security of the cloud

AWS infrastructure and services are also approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use AWS compliance 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 encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS 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 customers 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 information regarding the policies, processes, and controls established and operated by AWS. Customers can use this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.
- **Monitor,** through applicable security controls, that AWS maintains compliance with global standards and best practices.

AWS compliance programs

Certifications and third-party attestations

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

- **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 (ISMS) that defines how AWS continuously manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.
- **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 security controls implementation guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.
- **ISO 27018** – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It's 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 not addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.
- **ISO 27701** – ISO/IEC 27701 specifies requirements and guidelines to establish and continuously improve the Privacy Information Management System (PIMS), including processing of PII. It is an extension of the ISO/IEC 27001 and ISO/IEC 27002 standards for information security management providing a set of additional controls and associated guidance intended to address public cloud PIMS and PII management requirements for both processers and controllers, not addressed by the existing ISO/IEC 27002 control set. For more information, or to download the AWS ISO 27017 certification, see the ISO/IEC 27701 Compliance webpage.

- **ISO 22301** – ISO 22301 specifies requirements to implement, maintain and improve a business continuity management system (BCMS). The requirements specified in this standard are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size, and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity. The ISO 22301 standard is used to assess an organization's ability to meet its own business continuity needs and obligations. For more information, or to download the AWS ISO 22301 certification, see the ISO 22301 Compliance webpage.

- **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 where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, see the ISO 9001 Compliance webpage.

- **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 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 PCI Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.

- **SOC** – AWS System and Organization Controls (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 the SOC Compliance webpage. There are three types of AWS SOC Reports:

    - **SOC 1 Report**: 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 Security, Availability, Confidentiality and Privacy Report**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, confidentiality, and privacy.

    - **SOC 3 Security, Availability, Confidentiality and Privacy Report**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, confidentiality, and privacy without disclosing AWS internal information.

- For more information about other AWS certifications and attestations, see AWS Compliance Programs. For information about AWS security controls and service-specific security, see the Best Practices for Security, Identity, and Compliance website.

AWS Artifact

Customers can use AWS Artifact to review and download reports and details about more than 2,600 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

AWS Global infrastructure

The AWS Global Cloud infrastructure comprises AWS Regions and Availability Zones. A Region is a physical location in the world, consisting of multiple Availability Zones. An Availability Zone consists of one or more discrete data centers, each with redundant power, networking, and connectivity, all housed in separate facilities. Each zone has independent power, cooling, and physical security and is connected by redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple zones to achieve even greater fault-tolerance. You can learn more about these topics from the Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond whitepaper.

AWS customers choose the Regions in which their content and servers are located. This allows customers to establish environments that meet specific geographic or regulatory requirements. Additionally, this allows customers with business continuity and disaster recovery objectives to establish primary and backup environments in a location or locations of their choice. More information on our disaster recovery recommendations is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

Key regulations to consider

BSP is the central bank of the Republic of the Philippines. BSP aims to promote and maintain price stability, a strong financial system, and a safe and efficient payments and settlements system conducive to a sustainable and inclusive growth of the economy.

MORB and MORNBFI outline some of the regulations that BSFIs should consider when using cloud services. BSP updated some sections in MORB and MORNBFI that are relevant to use of cloud services by issuing Circular No. 1137 – Amendments to Outsourcing and IT Risk Management dated February 10, 2022 (Circular 1137).

This document provides some considerations for BSFIs as they assess their responsibilities under MORB and MORNBFI, including:

- **Section 112, MORB** – This section outlines the requirements that banks should assess compliance against in order to outsource banking functions.
- **Section 148, Appendix 78, MORB** – This appendix sets out guidelines for the vendor risk management programs that banks are required to establish when outsourcing banking functions.
- **Appendix 103, MORB, and Appendix Q-36, MORNBFI** – These appendices set out guidelines for banks and non-banks to notify BSP or obtain BSP approval for outsourcing arrangements.

- **Section 112-T, MORNBFI** – This section sets out the requirements that non-bank BSFIs should assess compliance against in order to outsource functions.

A full analysis of MORB and MORNBFI is beyond the scope of this guide. However, the following sections address the considerations that most frequently arise in interactions with BSFIs.

Section 112, MORB

Section 112-T, MORNBFI

Non-bank financial institutions regulated by BSP should consider Section 112, MORB, as the requirements might be applicable to them by virtue of Section 112-T, MORNBFI.

Approval and notification requirements

BSFIs should consider their Supervisory Assessment Framework (SAFr) rating, and whether their workloads are *material* workloads (see the following), when determining whether BSP approval is required for the BSFI to outsource the relevant workload. For more information on the SAFr rating system, see Circular 1137.

Depending on its SAFr rating, a BSFI might require BSP approval prior to outsourcing; if changes to an existing material outsourcing arrangement will significantly impact delivery of the outsourced service, business operations, reputation, or profitability; or if an existing outsourcing arrangement will become a material outsourcing arrangement.

Material outsourcing arrangements

BSFIs should make their own assessment of whether an outsourcing arrangement is material under BSP regulations. Amongst others, Section 1 of Circular 1137 clarifies that a material outsourcing arrangement is one that will significantly impact a BSFI's operations, financial condition, reputation, customers, and compliance with laws, rules, and regulations in the event of a business disruption to the outsourced activity, service delivery failure, data breach, or security breach of the outsourced workload. A list of factors that BSFIs should consider when determining whether an activity is material is included in Circular 1137.

Appendix 78, MORB

As amended by Circular 1137, Section 3 of Appendix 78 sets out some guidance that BSFIs should consider when designing an IT outsourcing or vendor risk management program for its technology service providers (TSP).

The following table outlines some AWS tools, services, and security, identity and compliance whitepapers that BSFIs might find relevant as they assess how to address the guidance in Appendix 78.

Excerpts of Appendix 78	Customer considerations
3.1 Risk Assessment. Prior to entering into an outsourcing plan, the BSFI should assess the risk of outsourcing…and establish appropriate measures to manage and control the identified risks… [*which*]…should take into consideration … the capability of the TSP and the technology it will use in delivering the outsourced service. (…)	AWS provides a wide range of information on its services and IT control environment on the AWS site and in whitepapers, reports, certifications, accreditations, and other third-party attestations. For further information on AWS, its services, and the benefits of the AWS Cloud, see the Overview of Amazon Web Services whitepaper or contact your AWS representative.
3.2 Service Provider Selection. Before selecting a service provider, the BSFI should perform appropriate due diligence of the provider's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity in relation to the services to be outsourced. (…)	Since 2006, AWS has provided flexible, scalable, and secure IT infrastructure to businesses of all sizes around the world. AWS has been continually expanding its services to support virtually any cloud workload and offers more than 200 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management. For more information on AWS services and the relevant technical documentation, see AWS Cloud Products and AWS documentation. 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 Amazon's Investor Relations website. A list of customer references and corresponding case studies can be found on the AWS Customer Success website.

Excerpts of Appendix 78	Customer considerations
***(3.2 continued)* For arrangements involving data transfer and handling, BSFIs should identify potential risks arising from physical and logical access of TSP employees, subcontractors, and other parties. As such, background checks on these companies are important to ensure that data are not being hosted by an organization that has a history or track record of not upholding confidentiality of information or that is engaging in malicious or fraudulent activity.**	In alignment with the ISO 27001 standard, AWS employees complete periodic role-based training that includes security training. Compliance audits are periodically performed to validate that employees understand and follow the established policies. See the AWS SOC Reports available on AWS Artifact for additional details. Where permitted by law, AWS requires that employees undergo a background screening at hiring, commensurate with their position and level of access. Personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Additionally, upon hire, personnel are required to read and accept the AWS Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics.
***(3.2 continued)* Business resilience and technical capability of the TSP in providing security and controls, audit and compliance, monitoring, and reporting requirements of the BSFI should also be carefully considered. (…)**	Customers can validate the implementation and effectiveness of security controls in place for information security of the cloud through AWS certifications and reports, including the AWS SOC 1, SOC 2, and SOC 3 reports, ISO 27001, ISO 27017, ISO 27018, ISO 27701, and ISO 22301 certifications and PCI DSS compliance reports. These reports and certifications are produced by independent third-party auditors.
3.3 Outsourcing Contracts. The contract (…) should be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, confidentiality and reporting. **a. Ensure the contract clearly defines the rights and responsibilities of both parties and contains (…) service level agreements;**	AWS offers an AWS Enterprise Agreement designed for BSFIs, together with an introductory guide to help customers assess the AWS Enterprise Agreement against BSP requirements. For more information about the AWS Enterprise Agreement, contact your AWS representative.

Excerpts of Appendix 78	Customer considerations
b. Ensure contracts with related entities clearly reflect an arms-length relationship(…); **c. Choose the most appropriate pricing method for the BSFI's needs;** **d. Ensure service provider's physical and data security standards meet or exceed the BSFI's standards. Any breach in security should be reported by the service provider to the BSFI;** **e. Engage legal counsel to review the contract; and** **f. Ensure the contract contains the minimum provisions required under existing Bangko Sentral rules and regulations (…).**	
3.4 Service Level Agreement (SLA). (…) Management should include SLAs in its outsourcing contracts to specify and clarify performance expectations, as well as establish accountability for the outsourced activity. (…) **SLAs addressing business continuity should measure the service provider's contractual responsibility for backup, record retention, data protection, and maintenance and testing of disaster recovery and contingency plans. (…)**	AWS commits to offer service level agreements (SLAs) and publish service level objectives (SLOs) for all paid, generally available services. AWS encourages customers to visit our well architected documentation for further details regarding SLOs. For further information about the AWS business continuity plan, see section 3.8 that follows.

Excerpts of Appendix 78	Customer considerations
3.5 Ongoing Monitoring ***3.5.1. Monitoring Program.*** **(…) [*The BSFI*] should establish a monitoring program to ensure service providers deliver the quantity and quality of services required by the contract. (…)**	The AWS Health Dashboard publishes up-to-the-minute information on service availability in AWS Regions around the world and a personalized view into the performance and availability of the services. Customers can use the AWS Security Bulletins website to keep updated on security announcements. AWS customers can also use the information available in near real-time monitoring and alerting services such as: • AWS CloudTrail to discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in an AWS account within a specified period of time. • Amazon CloudWatch to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. • Amazon GuardDuty to continuously monitor for malicious activity and unauthorized behavior to protect customer AWS accounts and workloads. Customers can also subscribe to AWS Support, which allows customers with operational issues or technical questions to contact a team of support engineers and receive personalized support. There are four types of support plans available. For more details, see Compare AWS Support Plans.
3.5.2. Financial Condition of Service Providers. **The BSFI should have an on-going monitoring of the financial condition of its service providers (…)**	See preceding section 3.2, customer considerations, for information about the financial status of Amazon.com.

Excerpts of Appendix 78	Customer considerations
3.5.3. General Control Environment of the Service Provider. **The BSFI should also implement adequate measures to ensure service providers are only given access to the information and systems that they need in order to perform their function. Management should restrict their access to BSFI's systems, and appropriate access controls and monitoring should be in place between the service provider's systems and the BSFI.**	AWS doesn't access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. For further information about some of the monitoring services available to customers, see section 3.5.5. that follows.
3.6 Security and Privacy. (…) BSFIs shall ensure that all confidential and sensitive data and information exposed to the TSP environment are well-managed and protected. (…) BSFIs shall likewise ensure that TSPs follow appropriate data handling procedures and employ robust access control mechanisms. (…)	Customers retain ownership and control of their content when using AWS services and have complete control over which services they use and whom they empower to access their content and services, including what credentials will be 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 doesn't change customer configuration settings, as these settings are determined and controlled by the customer. AWS customers have freedom to design their security architecture to meet their compliance needs. For further information about how customers can validate security controls in place for information security of the cloud, see the preceding section 3.2.

Excerpts of Appendix 78	Customer considerations
***(3.6 continued)* Moreover, BSFIs shall see to it that the TSP conducts periodic monitoring and reporting of security-related threats, incidents, and events on its networks/systems. The TSP should also have proactive incident response and problem management process in place, equipped with digital forensic tools and capabilities.**	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. Customers can evaluate the effectiveness of AWS-managed controls through audit reports and compliance evaluations available for free through AWS Artifact. See the following AWS Audit Reports for additional details: SOC 2, PCI DSS, ISO 27001, and ISO 27017.
***(3.6 continued)* In order to assess the TSP's ability to enforce appropriate technical, physical, and administrative safeguards (i.e., access controls, data segregation, etc.) across its organization, BSFIs may refer to independent assessments (e.g., external audit, security certificates, among others) which provide attestation on the effectiveness of the TSP's control environment and security mechanisms.**	AWS has implemented a formal audit program that monitors and audits controls that are designed to protect against organization risks and to protect customer data. This includes external independent assessments against regulatory, internal, and external control frameworks. Internal and external audits are planned and performed according to a documented audit schedule to review the continued performance of AWS against standards-based criteria, and to identify improvement opportunities. Standards-based criteria include, but are not limited to, the ISO 27001, Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 18), the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards, and the Payment Card Industry Data Security Standard PCI DSS 3.2.1. The AWS compliance team performs and reviews the audit plan according to the documented audit schedule and communicates the audit requirements based on standard criteria that verify compliance with the regulatory requirements and reported risk to the Audit Committee.

Excerpts of Appendix 78	Customer considerations
	Compliance reports from these assessments are made available through AWS Artifact to customers to enable them to evaluate the effectiveness of AWS-managed controls. See the following AWS Audit Reports for additional details: SOC 2, PCI DSS, ISO 27001, ISO 27017, and ISO 27018. The AWS Compliance reports identify the scope of AWS services and AWS Regions assessed, as well the assessor's attestation of compliance. Customers can perform vendor or supplier evaluations by using these reports and certifications. For more information about other AWS certifications and attestations, see the AWS Compliance Programs webpage. For information about general AWS security controls and service-specific security, see the Best Practices for Security, Identity, and Compliance website.
3.7 Data Ownership and Data Location and Retrieval. … BSFIs should be able to identify where the data is being processed and/or stored and assess whether the corresponding jurisdictions uphold data sovereignty laws.	Customers maintain control over their content and are responsible for choosing the country and the AWS Region where their customer content is stored. AWS will not move or replicate a customer's content outside of its chosen Regions without the customer's agreement, except as necessary to comply with the law or a binding order of a governmental body. For information on data privacy at AWS, visit the Data Privacy Center website.

Excerpts of Appendix 78	Customer considerations
***(3.7 continued)* BSFIs should ensure that ownership rights over its data must be clearly defined in the contract to establish the proper level of data access and control. At a minimum, the contract should contain the following provisions: i) the BSFI retains exclusive ownership over all of its data; ii) that TSP acquires no rights whatsoever to use the BSFI's data for its own purpose or for any purpose other than what is required based on the scope of service; and iii) the TSP does not have the right to prevent the duly authorized access of BSFI to its own data. (…)**	Customers retain ownership and control of their content when they use AWS services. 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 offers an AWS Enterprise Agreement designed for BSFIs, together with an introductory guide to help customers assess the AWS Enterprise Agreement against BSP requirements. For more information about the AWS Enterprise Agreement, contact your AWS representative.

Excerpts of Appendix 78	Customer considerations
3.8 Business Continuity Planning Consideration. The BSFI should integrate the TSP's BCP into its own plan, communicate functions to the appropriate personnel, and maintain and periodically review the combined plan. It should ensure that the TSP tests its plan annually and notify the institution of any resulting modifications. BSFIs shall likewise establish contingency plans in case the TSP becomes unavailable or inaccessible. Appropriate contingency and resumption strategies should be formulated to consider both short-term and prolonged unavailability/inaccessibility of the TSP.	AWS 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. AWS has obtained ISO 22301:2019 Compliance. The ISO 22301:2019 standard specifies requirements to implement, maintain, and improve a business continuity management system (BCMS). Additionally, the AWS Business Continuity plan details the process that AWS follows in 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, aiming to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions. 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 use of frequent server instance back-ups, data redundancy replication, and flexibility to place instances and store content within multiple AWS Regions as well as across multiple Availability Zones within each Region. In the case of failure, automated processes move customer content traffic away from the affected area. 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 supplies (UPS) and onsite backup generation facilities, Availability Zones are each fed by different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers.

Excerpts of Appendix 78	Customer considerations

Appendix 103, MORB and Appendix Q-36, MORNBFI

Appendices 103 and Q-36 (as amended by Circular 1137) set out:

- **Section A** – Information that should be maintained by BSFIs in relation to outsourcing arrangements and should be made available to BSP upon their request.
- **Section B** – Process for notifying BSP of new or altered material outsourcing arrangements that don’t require BSP approval.
- **Section C** – Process for applying for BSP approval, where required.

It is the BSFI’s responsibility to comply with the appendices.

Next steps

Each organization's cloud adoption journey is unique. To successfully complete your adoption, you need to understand your organization's current state, the target state, and the transition required to achieve the target state. Knowing this will help you set goals and create work streams that will enable staff to thrive in 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 within the framework can help you build a comprehensive approach to cloud computing across your organization throughout your IT lifecycle. The AWS CAF breaks down the complicated process of planning cloud adoption into manageable areas of focus.

Many organizations choose to apply the AWS CAF methodology with a facilitator-led workshop. To learn more about such workshops, contact your AWS representative. Alternatively, you can visit the webpage toaccess tools and resources for self-service application of the AWS CAF methodology.

For BSFIs in the Philippines, next steps typically also include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, AWS Solutions Architects, AWS Professional Services teams, and AWS Training instructors can assist with your cloud adoption journey. If you don't have an AWS representative, contact us.
- 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 through the AWS Management Console).
- Consider the relevance and application of the CIS AWS Foundations Benchmark, 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 for your due diligence and risk assessment, using the tools and resources referenced throughout this whitepaper and in the Additional Resources section that follows.
- Speak with your AWS representative about an AWS Enterprise Agreement.

Additional resources

For additional information, see:

- Using AWS in the Context of Philippines Privacy Considerations
- AWS Cloud Security Whitepapers and Guides

- AWS Compliance
- AWS Cloud Security Services
- AWS Best Practices for DDoS Resiliency
- AWS Cloud Security Checklist
- Cloud Adoption Framework – Security Perspective
- AWS Security Best Practices
- AWS Risk and Compliance
- AWS Compliance Center – Philippines

Contributors

Document revisions

Date	Description
December 22, 2023	First publication.