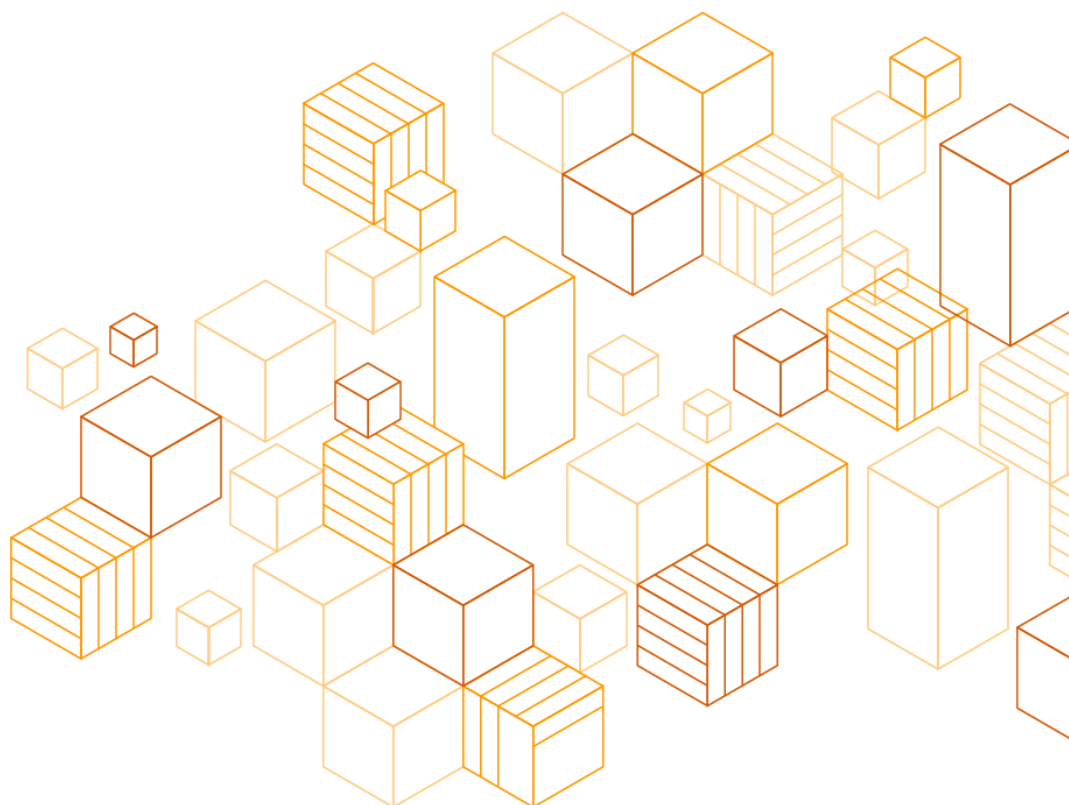


AWS User Guide to the Central Bank of Bahrain Rulebook

Outsourcing Operational Risk Management Module

Technical Guide

November 2020



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.

© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

About this Guide	vi
Overview	1
Security and the Shared Responsibility Model	2
Security IN the Cloud	3
Security OF the Cloud.....	4
AWS Compliance Assurance Programs	5
Certifications and Third-Party Attestations	5
AWS Artifact	7
AWS Global Infrastructure	8
Central Bank of Bahrain Rulebook on Outsourcing.....	8
Board and Senior Management Responsibilities	9
Notifications and Prior Approval Requests	9
Risk Assessment.....	10
Control Over Outsourced activities:.....	10
Customer Data Confidentiality:	10
Access to Information.....	11
Contingency Planning	11
Termination.....	12
Outsourcing Arrangements	12
Contingency Planning for Outsourcing Arrangements.....	12
Outsourcing of Functions Containing Customer Information	12
Next Steps	13
Additional Resources	14
Document Revisions.....	15
Appendix 1: AWS Considerations for the Technical and Operational Requirements under the CBB Rulebook on Outsourcing	16
OM-2.5 Outsourcing Agreement	17

Appendix 2: Due Diligence components.....	51
---	----

About this Guide

This AWS User Guide to the Central Bank of Bahrain Rulebook on Outsourcing Operational Risk guide provides information to assist financial institutions in the Kingdom of Bahrain that are regulated by the Central Bank of Bahrain (CBB) as they accelerate their use of Amazon Web Services (AWS) services.

This guide will provide the following information:

- Describe the respective roles that the customer and AWS each play in managing and securing the cloud environment.
- Provide an overview of the regulatory requirements and guidance that financial institutions can consider when using AWS.
- Provide additional resources that financial institutions can use to design and architect their AWS environment to be secure and meet regulatory expectations, including under CBB's regulations.

Overview

The Central Bank of Bahrain, in its capacity as the regulatory and supervisory authority for all financial institutions in the Kingdom of Bahrain (Bahrain), issues regulatory requirements that Licensees and other specified persons are legally obliged to comply with. These regulatory requirements are contained in the [CBB Rulebook](#).

The CBB Rulebook is relevant to the use of outsourced services and contains requirements for Conventional Bank Licensees (as such term is used in the CBB Rulebook, referred to throughout this guide as “Licensees”) operating in Bahrain on establishing parameters and control procedures to monitor and mitigate operational risks. References to AWS customer or Licensee appearing in this Guide may be used interchangeably, to the extent an AWS customer seeks to comply with its CBB requirements in its capacity as a Licensee.

This guide refers to certain rules applicable to Conventional Bank Licensees. While the equivalent rules applicable to other types of firms, such as insurers and advisers, are similar, in many respects the provisions will generally have some differences. Therefore, any financial institution should carefully assess whether the provisions highlighted in this guide are the same as those that apply to it when reviewing this guide. All firms operating in Bahrain must also consider any specific requirements issued by the CBB and any requirements that may override the commentary set out in this guide.

The following sections of the CBB Rulebook provide considerations for Licensees as they assess their responsibilities:

OM-2 Outsourcing: This section sets out the CBB's approach to outsourcing by Licensees. It also sets out various requirements that Licensees must address when considering outsourcing an activity or function, including the use of cloud services.

Taken together, Licensees can use this information to perform their due diligence and assess how to implement an appropriate information security, risk management, and governance program for their use of AWS. For a complete list of the CBB requirements, see the [CBB Rulebook](#).

This guide is intended to be a resource to help Licensees understand the technical and operational requirements under the [CBB Rulebook](#) when they use AWS services. This guide includes a description of the AWS compliance framework, advanced tools, and security measures, which Licensees can use to evaluate, meet, and demonstrate compliance with their applicable regulatory requirements under the [CBB Rulebook](#).

This guide focuses on typical security-related questions asked by AWS customers when considering the [CBB Rulebook](#) and their use of AWS services. It does not cover every provision of the CBB Rulebook, nor does it address other compliance or legal requirements that may apply to customers. This document is provided for informational purposes only; it is not legal advice and should not be relied on as legal advice. As customers' requirements will differ, AWS encourages its customers to obtain appropriate advice on their compliance with all regulatory and legal requirements that are relevant to their business, including the CBB Rulebook and local regulations and laws.

Security and the Shared Responsibility Model

It is important that Licensees understand the [AWS Shared Responsibility Model](#) before exploring the specific technical and operational requirements outlined in the CBB Rulebook. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS for security, and informs the steps Licensees need to take to ensure they comply with the CBB Rulebook.

Cloud security is a shared responsibility. AWS manages security of the cloud by ensuring that AWS Cloud Infrastructure complies with global and regional regulatory requirements and best practices, but security in the cloud is the responsibility of the customer.

This means that customers retain control of the security program they choose to implement to protect their own content, platform, applications, systems, and networks, just as they would for applications in an on-premises data center.

The 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 AWS services operate.

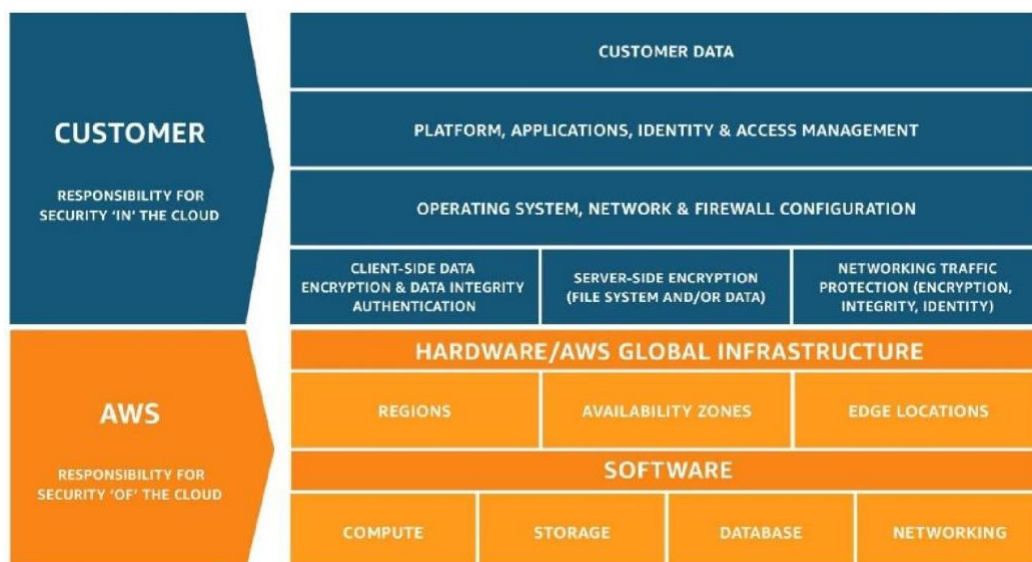


Figure 1 – Shared Responsibility Model

Security IN the Cloud

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

It is 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 will be determined by the AWS services that a customer selects. This 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) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks.

Customers that deploy an Amazon 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 abstracted AWS 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 data. Whether the customer is using IaaS or an abstracted service, customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

Security OF the Cloud

AWS's infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use AWS's compliance certifications to validate the implementation and effectiveness of AWS's security controls, including internationally-recognized security best practices and certifications. Customers can learn more by downloading the [AWS & Cybersecurity in the Financial Services Sector](#) whitepaper.

The AWS compliance program is based on the following actions:

- **Validation** 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.

- **Demonstrating** 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.
- **Monitoring** through applicable security controls, that AWS maintains compliance with global standards and best practices.

AWS Compliance Assurance Programs

This program has obtained certifications and third-party attestations for a variety of industry-specific workloads. AWS has also developed compliance programs to make these resources available to customers. Additionally, the CBB has added Section - OM - 2.5.2 to the rulebook on January 2020. This section outlines the Licensee's options in assessing an outsourcing service provider, including review of independent third-party certifications, third party audit or internal audit reports. Customers can leverage the AWS compliance programs to help satisfy their regulatory requirements. For more information about these third-party certifications and audit reports, see the [AWS Compliance Programs](#) webpage.

Certifications and Third-Party Attestations

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

- **ISO 27001**: 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 that defines how AWS perpetually 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:** 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:** 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 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 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 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/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 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:** Provides information about the AWS control environment that may 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 with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
 - **SOC 3:** Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality, without disclosing AWS internal information.

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

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 [Amazon Web Services: Overview of Security Processes](#) whitepaper.

AWS Artifact

Customers can review and download reports and details about more than 2,600 security controls by using [AWS Artifact](#), the automated compliance reporting portal available in the AWS Management Console. 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.

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 applications and databases which are more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment. Customers can learn more about these topics by downloading our Whitepaper on [Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond](#).

AWS customers can choose the AWS Region(s) in which their content and servers are located. This enables customers to establish environments that meet specific geographic or regulatory requirements. Additionally, this enables 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 [AWS Disaster Recovery](#).

AWS customers can use the AWS Global Cloud Infrastructure to design an AWS environment consistent with their business and regulatory needs, including any applicable requirements under the CBB Regulation.

Central Bank of Bahrain Rulebook on Outsourcing

This section sets out common considerations for Licensees that use AWS as they consider some of the key technical and operational requirements under the CBB Regulation, and describes how Licensees can leverage AWS services and tools to comply with their applicable regulatory requirements. Appendix: 1 Considerations for the CBB Rulebook Requirements provides a list of requirements and corresponding considerations.

Licensees that use the cloud are expected to carry out due diligence, evaluate and address risks, and enter into appropriate outsourcing agreements. Appendix 1 – Considerations for the Technical and Operational Requirements in the CBB Rulebook on Outsourcing. The tables in the appendix address the following:

- **Requirement:** This column lists the minimum technical and operational requirements (per category) that may be applicable to each of the scenarios outlined in the CBB Rulebook.
- **Considerations:** This column explains the considerations for addressing the requirements defined by the CBB Rulebook. It may refer to the security and compliance of the cloud, and how AWS implements and manages the controls and/or AWS services Licensees can use to address these requirements.
- **Well-Architected framework considerations:** This column lists best practices for security in the cloud from the AWS Well-Architected Framework that Licensees can implement as a starting point to support their compliance efforts. Details on each best practice and associated AWS services that customers may leverage can be found in the AWS Well-Architected Framework.

The [Operational Risk Management Module](#) (OM) of the CBB Rulebook sets out the Central Bank of Bahrain's rules and guidance to Licensees operating in Bahrain on establishing parameters and control procedures to monitor and mitigate operational risks. The [Outsourcing Chapter](#) (OM-2) sets out the CBB's approach to outsourcing by Licensees. It also sets out various requirements that Licensees must address when considering outsourcing an activity or function, including use of cloud services by Licensees.

Under Section OM-2.1, the CBB Rulebook details the approach to outsourcing by Licensees. It is the Licensee's responsibility to address specific requirements when considering outsourcing an activity or function, including but not limited to requirements for material outsourcing and various factors to be considered when assessing a material outsourcing function, activity, or process.

Board and Senior Management Responsibilities

Under Section OM-2.2, it is the Licensee's board of senior management's responsibility to understand the operational and reputational risks associated with outsourcing arrangements and to ensure that effective risk management policies, procedures and practices are in place to manage the risks in outsourcing activities (Appendix 2 – Due Diligence).

Notifications and Prior Approval Requests

Under Section OM-2.3, it is the Licensee's responsibility to seek the CBB's prior written approval before committing to a new material outsourcing agreement. In general, the

request for prior approval must be made six weeks before the Licensee intends to commit to the outsourcing arrangement.

Risk Assessment

Under Section OM-2.4, Licensees must undertake a thorough risk assessment of an outsourcing proposal, before formally submitting the request for approval to the CBB and committing itself to an agreement. AWS gives customers ownership and control over their content by design, through tools that allow customers to determine where their content will be stored, how it will be secured in transit or at rest, and how access to their AWS environment will be managed. AWS has implemented global privacy and data protection best practices in order to help customers establish, operate and leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments. While each AWS customer is responsible for executing against their own internal risk activities and posture, [AWS Professional Services](#) can be engaged to assist in the implementation of controls determined by customers

Control Over Outsourced activities:

Under Section OM-2.5.1.a, Licensees need to ensure that they have sufficient and effective procedures for monitoring the performance of the service provider, the relationship with the service provider and the risks associated with the outsourced activity. While customers are ultimately responsible for establishing a governance framework and monitoring their own environments, AWS provides many tools to help customers efficiently achieve compliance with applicable regulatory requirements, including the CBB Rulebook.

Customer Data Confidentiality:

Under Section OM-2.5.1.b, Licensees need to ensure that as part of the outsourcing, Licensees can continue to comply with local and regional data protection requirements. Security remains AWS's highest priority, and AWS continues to innovate and invest in a high bar for security and compliance across all global operations. Licensees retain ownership and control of their data when using AWS services. Licensees have complete control over which AWS services they use and who they empower to access their content and AWS services, including what credentials will be required. Licensees control how they configure their environments and secure their data, including whether they encrypt their data (at rest and in transit), and what other security features and tools

they use and how they use them. AWS does not change Licensee's configuration settings, as these settings are determined and controlled by Licensee.

- **Data Protection:** Licensees choose how their data is secured. AWS offers strong encryption for data in transit or at rest, and AWS provides Licensees with the option to manage their own encryption keys. For further details, see the [AWS Key Management Service Cryptographic Details](#) whitepaper.
- **Data Integrity:** For access and system monitoring, [AWS Config](#) provides Licensees with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. AWS Config enables Licensees to create rules that automatically check the configuration of AWS resources recorded by AWS Config. AWS Config represents relationships between resources, so that Licensees can assess how a change to one resource might impact other resources.
- **Data Segregation:** The [Logical Separation Handbook](#) will help Licensees understand logical separation in the cloud and demonstrates its advantages over a traditional physical separation model. [Amazon Virtual Private Cloud](#) (Amazon VPC) lets Licensees provision a logically isolated section of the AWS Cloud where Licensees can launch AWS resources in a virtual network that they define.

Access to Information

Under Section 2.5.1.c, Licensee's outsourcing arrangements should not interfere with the ability of the Licensee to effectively manage its business activities or impede the CBB in carrying out its supervisory functions and objectives. AWS provides a number of ways for Licensees to identify users and securely access their AWS accounts. AWS also provides additional security options that enable Licensees to further protect their AWS accounts and control access using [AWS Identity and Access Management](#) (IAM), key management and rotation, temporary security credentials, and multi-factor authentication (MFA).

Contingency Planning

Under Section 2.5.1.d, Licensees should ensure that they have an adequate understanding of their service provider's contingency plan and consider implications for their own contingency planning in the event that the outsourced service is interrupted.

Termination

Under Section 2.5.1.e, in the event of a termination of an outsourcing agreement, for whatever reason, Licensee should ensure that all customer data is retrieved from the service provider. AWS provides Licensees with the ability to delete their data. Because Licensees retain control and ownership of their data, it is the Licensee's responsibility to manage data retention to its own requirements. If a Licensee decides to leave AWS, it can manage access to its data and AWS services and resources, including the ability to import and export data.

Outsourcing Arrangements

Under Section OM - 2.5.2 to the rulebook on January 2020. This section outlines the Licensee's options in assessing an outsourcing service provider, including review of independent third-party certifications, third-party audit, or internal audit reports

Contingency Planning for Outsourcing Arrangements

Under Section 2.6, Licensee should maintain and regularly review contingency plans (detailed guidance in OM-4). AWS provides Licensee with the capability to implement a robust continuity plan, including frequent server instance backups, 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 disaster recovery approaches, see [Disaster Recovery](#).

Outsourcing of Functions Containing Customer Information

Under Section 2.8, because of the critical importance of protecting customer information confidentiality, all proposals to outsource functions containing customer information should be considered material, and controls set accordingly. Customers manage access to their customer content and AWS services and resources. We offer our customers strong encryption for customer content in transit or at rest, and we provide customers with the option to manage their own encryption keys. AWS offers numerous services to customers to enable them to track, monitor, analyze, and audit events.

Next Steps

Each organization's cloud adoption journey is unique. In order to successfully execute a cloud adoption, Licensees need to understand their organization's current state, the target state, and the transition required to achieve the target state. Knowing this will help Licensees 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 Licensees build a comprehensive approach to cloud computing across their organization, throughout the IT lifecycle. The AWS CAF breaks down the complicated process of planning into manageable areas of focus.

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

For Licensees regulated by the CBB, next steps typically also include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, as well as AWS Solution Architects, Professional Services teams, and Training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please [contact us](#).
- Obtain and review a copy of the latest AWS SOC 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification, from the [AWS Artifact](#) portal (accessible via the AWS Management Console).
- Consider the relevance and application of the CIS AWS Foundations Benchmark available [here](#) and [here](#), as appropriate for your cloud journey and use cases. These industry-accepted best practices published by the Center for Internet Security go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.

- Dive deeper on other governance and risk management practices as necessary in light of your due diligence and risk assessment, using the tools and resources referenced throughout this whitepaper and in the [Additional Resources](#) section below.
- Speak with your AWS representative to learn more about how AWS is helping financial services customers migrate their critical workloads to the cloud.

Additional Resources

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

- [AWS Compliance Quick Reference Guide](#): AWS has many compliance-enabling features that you can use for your regulated workloads in the AWS cloud. These features allow you to achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry, easier operations, and improved agility by providing more oversight, security control, and central automation.
- [AWS Well-Architected Framework](#): The Well-Architected framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. AWS has produced whitepapers addressing each pillar of the Well-Architected Framework, that are available here: [AWS Operational Excellence Pillar Whitepaper](#); [AWS Security Pillar Whitepaper](#); [AWS Reliability Pillar Whitepaper](#); [AWS Performance Efficiency Whitepaper](#); [AWS Cost Optimization Whitepaper](#), [AWS Operational Resilience Whitepaper \(March 2019\)](#), [Data Classification and Secure Cloud Adoption Whitepaper \(June 2018\)](#), and [AWS Policy Perspectives: Data Residency \(July 2018\)](#).
- [Global Financial Services Regulatory Principles](#): AWS has identified five common principles related to financial services regulation that customers should consider when using AWS cloud services and specifically, applying the shares responsibility model to their regulatory requirements. Customers can access a whitepaper on these principles under a non-disclosure agreement at [AWS Artifact](#).

- NIST Cybersecurity Framework (CSF): The AWS whitepaper [NIST Cybersecurity Framework \(CSF\): Aligning to the NIST CSF in the AWS Cloud](#) demonstrates how public and commercial sector organizations can assess the AWS environment against the NIST CSF and improve the security measures they implement and operate (i.e., security in the cloud). The whitepaper also provides a third-party auditor letter attesting to the AWS cloud offering's conformance to NIST CSF risk management practices.
- [Using AWS in the Context of Common Privacy and Data Protection Considerations](#): This document provides information to assist customers who want to use AWS to store or process content containing personal data, in the context of common privacy and data protection considerations. It will help customers understand the way AWS services operate, including how customers can address security and encrypt their content. The geographic locations where customers can choose to store content and other relevant considerations.
- [Payment Card Industry Data Security Standard \(PCI DSS\) 3.2.1 on AWS](#): This guide provides customers with sufficient information to be able to plan for and document the Payment Card Industry Data Security Standard (PCI DSS) compliance of their AWS workloads.
- [AWS Answers to Key Compliance Questions \(January 2017\)](#): This document addresses common cloud computing compliance questions as they relate to AWS. The answers to these questions may be of interest when evaluating and operating in a cloud computing environment and may assist in AWS customers' control management efforts.
- [AWS Risk and Compliance \(May 2017\)](#): This document is intended to provide information to assist AWS customers with integrating AWS into their existing control framework supporting their IT environment. This document includes a basic approach to evaluating AWS controls and provides information to assist customers with integrating control environments.

For additional help visit the [Security, Identity and Compliance Whitepapers](#).

Document Revisions

Date	Description
November 2020	First publication

Appendix 1: AWS Considerations for the Technical and Operational Requirements under the CBB Rulebook on Outsourcing

The following sections list the technical and operational requirements identified under Sections 2.5, 2.6 and 2.8 of the [CBB Rulebook](#) along with AWS considerations to assist Licensees understand each requirement when using AWS, and a description of the best practices from the [AWS Well-Architected Framework](#) which Licensees can use to support their compliance efforts.

The AWS Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars—operational excellence, security, reliability, performance efficiency, and cost optimization—the Framework provides a consistent approach for customers to evaluate architectures, and implement designs that will scale over time.

The tables in the next sections are organized into the following columns:

- **Requirement:** This column lists the minimum technical and operational requirements (per category) that may be applicable to each of the scenarios outlined in the CBB Rulebook.
- **AWS Considerations:** This column explains the AWS considerations for addressing the requirements defined by the CBB Rulebook. It may refer to the security and compliance of the cloud, and how AWS implements and manages the controls and/or AWS services Licensees can use to address these requirements.
- **Implementation Considerations:** This column lists best practices for security in the cloud from the AWS Well-Architected Framework that Licensees can implement as a starting point to support their compliance efforts. Details on each best practice and associated AWS services that customers may leverage can be found in the AWS Well-Architected Framework.

The following tables provide additional considerations on how customers can support their compliance efforts of their applicable requirements under the CBB Rulebook. These tables contain only a non-exhaustive sample of considerations. This is not legal or compliance advice. Customers should consult with their own legal and compliance teams.

OM-2.5 Outsourcing Agreement

OM-2.5.1.a Control Over Outsourced activities

CBB Rulebook Section - OM-2.5.1.a Requirement	Considerations	Well-Architected framework considerations
<p>1. The Board and management of Licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in outsourced activities. Licensees must therefore ensure that they have adequate mechanisms for monitoring the performance of, and managing the relationship with, the outsourcing service provider.</p>	<p>Customer Responsibility</p> <p>While customers are ultimately responsible for establishing a governance framework and monitoring their own environments, AWS provides many tools to help customers efficiently achieve compliance with applicable regulatory requirements, including the CBB Rulebook.</p> <p>AWS has implemented a formal, documented incident response policy and program which can be reviewed in the SOC 2 report via AWS Artifact. Licensees can also see security notifications on the AWS Security Bulletins website. AWS provides Licensees with various tools Licensees can use to monitor the AWS services, including those already noted and others on the AWS Marketplace.</p> <p>For example, AWS Config enables customers to continuously monitor and record their AWS resource configurations, and automatically evaluate the recorded configurations against the desired configurations. Amazon CloudWatch allows customers to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. With the Personal Health Dashboard, changes in the health of AWS resources automatically trigger alerts, providing event visibility and guidance to help quickly diagnose and resolve issues. Customers can use these alerts to react and keep their applications running smoothly.</p>	<p>SEC-4 Detect and investigate security events</p> <p>REL-6 Monitor workload resources</p> <p>PERF-7 Monitor resources to ensure they are performing as expected</p>

CBB Rulebook Section - OM- 2.5.1.a Requirement	Considerations	Well-Architected framework considerations
<p>2. A service level agreement (“SLA”) – setting out the standards of service to be provided – must form part of the outsourcing agreement. Where the outsourcing provider interacts directly with a Licensee’s customers, the SLA must – where relevant – reflect the Licensee’s own standards and the CBB’s relevant rulebook requirements regarding customer service.</p>	<p>Shared Responsibility</p> <p>AWS offers service level agreements for certain AWS services. These may be updated from time to time.</p>	<p>OPS-2 structure your organization to support your business outcomes</p>
<p>3. Mechanisms for the regular monitoring by Licensees of performance against the SLA and other targets, and for implementing remedies in case of any shortfalls, must also form part of the agreement.</p>	<p>Shared Responsibility</p> <p>AWS provides up-to-the-minute information on the health of AWS services at the publicly available Service Health Dashboard. In addition, customers can configure a personalized Health Dashboard to receive a personalized view of the performance and availability of the AWS services underlying their resources and applications. These dashboards display relevant and timely information to help customers manage events in progress, and provide proactive notification to help customers plan for scheduled activities. With the Personal Health Dashboard, changes in the health of AWS resources automatically trigger alerts, providing event visibility and guidance to help quickly diagnose and resolve issues. Customers can use these alerts to react and keep their applications running smoothly.</p>	<p>OPS-2 structure your organization to support your business outcomes</p> <p>OPS-10 manage workload and operations events</p> <p>REL-6 Monitor workload resources</p> <p>REL-11 Design workload to withstand component failures</p> <p>PERF-7 Monitor resources to ensure they are performing</p>

CBB Rulebook Section - OM-2.5.1.a Requirement	Considerations	Well-Architected framework considerations
4. Clear reporting and escalation mechanisms must be specified in the agreement.	<p>Shared Responsibility:</p> <p>AWS considers the development and implementation of mechanisms and plans to detect, respond and manage information security incidents as a shared responsibility between AWS and AWS customers regulated by CBB.</p> <p>Customers' information security response plans must include the mechanisms for managing all relevant stages of an incident including escalation and reporting. Customers must annually review and test their information security response plans to ensure they remain effective and fit-for-purpose.</p> <p>AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, Security Hub, and AWS Config Rules to track, monitor, analyze, and audit events. If these tools identify an event that is analyzed and determined to be an incident, that "qualifying event" will raise an incident and trigger the incident management process and any appropriate response actions necessary to mitigate the incident.</p>	<p>OPS-2 structure your organization to support your business outcomes</p> <p>OPS-3 Support your organizational culture</p> <p>OPS-10 manage workload and operations events</p> <p>SEC-4 Detect and investigate security events</p> <p>SEC 10: How do you anticipate, respond to, and recover from incidents?</p>
5. Where an outsourcing service provider in turn decides to sub-contract to other providers, the Licensee must perform a due diligence and a risk and control assessment and obtain CBB's prior written approval.	<p>Customer Responsibility</p> <p>AWS operates a global, one-to-many service model and may potentially sub-outsource certain functions to other service providers. If AWS sub-outsources to another service provider, AWS will comply with the applicable requirements of the CBB Rulebook on sub-contracting.</p> <p>A list of any subcontractors whose role is such that its failure to perform would have a significant effect on AWS's ability to provide services to its customers in accordance with AWS's obligations can be accessed here: https://aws.amazon.com/compliance/chain-subcontractors/.</p>	Not applicable.

CBB Rulebook Section - OM-2.5.1.a Requirement	Considerations	Well-Architected framework considerations
6. In case of (5) above, the original provider must remain contractually liable to the Licensee for the quality and level of service agreed, and its obligations to the Licensee must remain unchanged.	<p>Shared Responsibility</p> <p>The use of subcontractors will not release AWS from any of its obligations under the agreement between Licensee and AWS.</p> <p>A list of any subcontractors whose role is such that its failure to perform would have a significant effect on AWS's ability to provide services to its customers in accordance with AWS's obligations can be accessed here: https://aws.amazon.com/compliance/chain-subcontractors/.</p>	Not applicable.

OM-2.5.1.b Customer data confidentiality

CBB Rulebook Section - OM - 2.5.1.b	Well-Architected framework considerations
Requirement	Considerations
1. Licensees must ensure that outsourcing agreements comply with the requirements of Law No. 30 of 2018, Personal Data Protection Law (PDPL) issued on 12 July 2018, as applicable, and other applicable legal requirements regarding customer confidentiality.	<p>Shared Responsibility</p> <p>Our industry-leading functionality provides the foundation for our long list of internationally-recognized certifications and accreditations, demonstrating compliance with rigorous international standards, such as ISO 27001 for technical measures, ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, and PCI DSS Level 1. AWS continues to pursue the certifications that assist our customers.</p> <p>As explained in the AWS Shared Responsibility Model, it is important to note that when using AWS services, customers maintain control over their data and are responsible for managing critical content security requirements. This allows customers to control the entire life-cycle of their content on AWS and manage</p>

their content in accordance with their own specific needs, including content classification, access control, retention, and deletion.

For more information about the Shared Responsibility Model and its implications for the storage and processing of personal data using AWS, see the AWS whitepaper [Using AWS in the Context of Common Privacy and Data Protection Considerations](#)

Pursuant to the PDPL, Licensees should also consider consent requirements for the storage of personal data outside Bahrain when using AWS services. Where consent of customers is used, arrangements may need to be considered in the event such customer revokes its consent under the PDPL.

AWS offers services and resources to our customers to help them comply with data protection requirements that may apply to their activities. AWS maintains a systematic approach to planning and developing new services for the AWS environment to ensure that the quality and security requirements are met with each release. New features are launched regularly, and AWS has 500+ features and services focused on security and compliance.

In addition, all AWS services can be used in compliance with the GDPR. This means that, in addition to benefiting from all of the measures that AWS already takes to maintain services security, customers can deploy AWS services as a key part of their GDPR compliance plans.

2. Licensees must ensure that the outsourcing service provider implements adequate safeguards and procedures. Amongst other things, customer data must be properly segregated from those belonging to other clients the outsourcing service provider may have.

Shared Responsibility

The [Logical Separation Handbook](#) will help Licensees understand logical separation in the cloud and demonstrates its advantages over a traditional physical separation model. [Amazon Virtual Private Cloud](#) (Amazon VPC) lets Licensees provision a logically isolated section of the AWS Cloud where Licensees can launch AWS resources in a virtual network that they define.

Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Licensees maintain full control over who has access to their data.

SEC-1 Operate workload securely

REL-2 Plan network topology

AWS services which provide virtualized operational environments to customers (i.e., EC2) ensure that customers are segregated from one another and prevent cross-tenant privilege escalation and information disclosure via hypervisors and instance isolation.

Different instances running on the same physical machine are isolated from each other via the hypervisor. In addition, the Amazon EC2 firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer; thus, an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical random-access memory (RAM) is separated using similar mechanisms.

Customer instances have no access to physical disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically erases every block of storage before making it available for use, which protects one customer's data from being unintentionally exposed to another. Customers can further protect their data using traditional filesystem encryption mechanisms, or, in the case of [Amazon Elastic Block Store](#) (Amazon EBS) volumes, by enabling AWS-managed disk encryption.

A Dedicated Host is also a physical server that's dedicated for customer use. With a Dedicated Host, customers have visibility and control over how hypervised instances are placed on the server. Bare metal instances are non-hypervised host hardware devices. Using the [AWS Nitro](#) technology for network and storage offload, as well as the Nitro security chip to eliminate the risks associated with serial single-tenancy on bare metal, customers have direct access to Amazon EC2 hardware. These bare metal instances are full-fledged members of the Amazon EC2 service and have access to AWS services such as [Amazon VPC](#) and [Amazon Elastic Block Store \(EBS\)](#).

3. Customer information must be encrypted and Licensees must ensure that all encryption keys or similar forms of authentication are kept secure within the Licensee's control.

Shared Responsibility

[AWS Key Management Service](#) (AWS KMS) allows customers to create and manage cryptographic keys and control their use across a wide range of AWS services and in their applications. AWS KMS is a secure and resilient service that uses hardware security modules that

[SEC-7](#) Identify and classify data
[REL-9](#) Secure and encrypt backups

have been validated under FIPS 140-2, or are in the process of being validated, to protect customer keys. AWS KMS is integrated with [AWS CloudTrail](#) to provide customers with logs of all key usage. For further details please see the AWS Whitepaper: [AWS Key Management Service Cryptographic Details](#).

4. **Outsourcing service providers must give suitable undertakings that the company and its staff will comply with all applicable confidentiality rules. Licensees must have contractual rights to take action against the service provider in the event of a breach of confidentiality.**

Shared Responsibility

Not Applicable

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 data. Maintaining customer trust and confidence is of the utmost importance to AWS. Any breach of AWS's obligations can be pursued by the Customer under the terms of their agreement with AWS.

5. **Licensees must assess the impact of using an overseas-based outsourcing service provider on their ability to maintain customer data confidentiality, for instance, because of the powers of local authorities to access such data.**

Customer Responsibility

AWS customers designate in which geographic region their content will be located. With AWS, Licensees can: (1) Determine where their content will be stored, including the type of storage and geographic region of that storage, (2) Replicate and back up their content in more than one region, and AWS will not move or replicate customer outside of the licensee's chosen region(s), except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users. For current information on AWS Regions and Availability Zones, see [Global Infrastructure](#), and choose the secured state of their content. We offer customers strong encryption for content in transit or at rest, and we provide them with the option to manage their own encryption keys. If Licensees want to tokenize data before it leaves their organization, Licensees can engage a number of AWS partners with relevant expertise. For more information about Key Management Service see [KMS](#), and about cloud-based Hardware security module see [CloudHSM](#).

[SEC-7](#) Identify and classify data

[SEC-8](#) Protect data at rest

[SEC-9](#) Protect data in transit

[REL-9](#) – Secure and encrypt backups

Manage access to their content and AWS services and resources through users, groups, permissions and credentials that customers' control.

Licensees should consider the relevant restrictions on overseas storage of personal data and relevant consent requirements under the PDPL.

OM-2.5.1.c Access to information

CBB Rulebook Section - OM - 2.5.1.c.1		Well-Architected framework considerations
Requirement	Considerations	
Outsourcing agreements must ensure that the Licensee's internal and external auditors have timely access to any relevant information related to the outsourced function/service they may require to fulfill their responsibilities. Such access must allow them to conduct on-site examinations of the relevant function/service provided by outsourcing service provider, if required.	<p>Shared Responsibility</p> <p>Customers have root access or administrative control over their accounts, services, and applications. The AWS services provide customers with complete visibility of their cloud resources, services and applications to monitor use and log, collect metrics, set alarms, and automatically react to changes.</p> <p>Additionally, customers can validate the security controls in place within the AWS environment through AWS certifications and reports, such as ISO 27001 for technical measures ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, and PCI DSS Level 1. These reports and certifications are produced by independent third-party auditors and attest to the design and operating effectiveness of AWS security controls.</p> <p>Customers can use AWS Artifact, the automated compliance reporting portal available in the AWS Management Console, to review and download reports and details about the AWS 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.</p>	<p>OPS-1 Determine priorities</p> <p>OPS-7 Ensure consistent review of operational readiness</p> <p>SEC-1 Operate workload securely</p> <p>SEC-7 Identify and classify data</p>

AWS 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 general improvement opportunities. Standards-based criteria includes, but is not limited to the ISO/IEC 27001, the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements (SSAE) 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards.

Additionally, the CBB has added Section - OM - 2.5.2 to the rulebook on January 2020. This section outlines the Licensee's options in assessing an outsourcing service provider, including review of independent third-party certifications, third party audit or internal audit reports. For more information about these third-party certifications and audit reports, see the [AWS Compliance Assurance Programs](#) webpage.

CBB Rulebook Section - OM - 2.5.1.c.4		Well-Architected framework considerations
Requirement	Considerations	
The outsourcing service provider must commit itself, in the outsourcing agreement, to inform the Licensee of any developments that may have a material impact on its ability to meet its obligations. These may include, for example, relevant control weaknesses identified by the outsourcing service provider's	<p>Shared Responsibility</p> <p>AWS provides ongoing reporting to customers through the AWS Personal Health Dashboard, which provides proactive notifications and displays relevant and timely information to help customers manage events in progress. Alerts in the AWS Personal Health Dashboard are automatically triggered by changes in the health of AWS resources, giving customers event visibility, and guidance to help quickly diagnose and resolve issues.</p> <p>With regard to AWS's incident management, AWS adheres to industry best practices, including but not limited to the following activities: notifying operational and management personnel of incidents when early warning</p>	<p>OPS-3 Support your organizational culture</p> <p>OPS-7 Ensure consistent review of operational readiness</p> <p>OPS-10 Manage workload and operations events</p> <p>SEC-4 Detect and investigate security events</p>

internal or external auditors, and material adverse developments in the financial performance of the outsourcing service provider.	<p>thresholds are crossed on key operational metrics, logging system activities for forensic analysis, and conducting post-mortems.</p> <p>AWS also offers numerous services to customers to enable them to track, monitor, analyze, and audit events. For example, customers can use AWS CloudTrail, Amazon CloudWatch, AWS Config, and AWS Config Rules, among other services and tools. Another service, AWS Trusted Advisor, helps customers reduce cost, increase performance, and improve security through real-time guidance that follows AWS best practices. Additionally, see considerations related to Section 2.5.1.c.3</p>	SEC-4 Detect and investigate security events
---	--	---

OM-2.5.1.d Contingency Planning

CBB Rulebook Section - OM - 2.5.1.d		Well-Architected framework considerations
Requirement	Considerations	
1. Licensees must ensure that service providers regularly review and test plans to ensure continuity in the provision of the outsourced service.	<p>Customer Responsibility</p> <p>The AWS Business Continuity policy lays out the guidelines used to implement procedures to respond to a serious outage or degradation of AWS services, including the recovery model and its implications on the business continuity plan. 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. Customers are responsible for establishing and testing their own business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.</p> <p>Licensees should consider the relevant restrictions on any overseas storage personal data in any continuity/back-up plans and any consent requirements under the PDPL. See the additional information provided and referred to at Section OM - 2.5.1.b above.</p>	REL-9 Secure and encrypt backups

2. Licensees must have an adequate understanding of the outsourcing service provider's arrangements, to understand the implications for its own contingency arrangements (see Section OM-2.6).

Customer Responsibility

AWS and regulated AWS Customers share a common interest in maintaining operational resilience, i.e., the ability to provide continuous service despite disruption. Continuity of service, especially for critical economic functions, is a key prerequisite for financial stability. For more information about AWS operational resilience approaches, see the AWS whitepaper: [Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond](#). 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. For more information, see the AWS whitepaper: [Amazon Web Services: Overview of Security Processes](#) and the SOC 2 report in the [AWS Artifact](#) console.

[REL-9](#) Secure and encrypt backups

OM-2.5.1.e Termination

CBB Rulebook Section - OM - 2.5.1.e	
Requirement	Considerations
1. Licensees must have the right to terminate the agreement should the outsourcing service provider undergo a change of ownership (whether direct or indirect) that poses a potential conflict of interest; becomes insolvent; or goes into liquidation or administration.	<p>Shared Responsibility</p> <p>The AWS Customer Agreement (as updated from time to time) allows customers the ability to terminate their use of AWS's services for convenience at any time and for any reason.</p>
2. Termination under any other circumstances allowed under the agreement must give Licensees a sufficient notice period in which they can affect a smooth transfer of the service to another provider or bring it back in-house.	<p>Shared Responsibility</p> <p>AWS offers customers services that can be used to design an exit strategy for services that are internally compatible or externally transferable. For example, AWS Simple Storage Service (S3) and Glacier customers only need to consider how they will export their objects from the services. AWS offers several ways to export customer data, including a large storage appliance service called Snowball. Additionally, AWS offers AWS Database Migration Service, a web service that Licensees can use to migrate a database from an AWS service to an on-premises database.</p> <p>Because Licensees retain control and ownership of their data, it is the Licensee's responsibility to manage data retention to its own requirements. If a Licensee decides to leave AWS, it can manage access to its data and AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Import/Export to transfer large amounts of data into and out of AWS using physical storage appliances. For more information, see Cloud Storage with AWS.</p>
3. In the event of termination, for whatever reason, the agreement must provide for the return of all customer data where required by Licensees.	<p>Shared Responsibility</p> <p>AWS services enable the export of content by customers on demand, using the AWS Management Console, APIs, and other methods. For example, AWS Snowball provides devices designed to be secure to transfer large amounts of data into and out of the AWS services. For more information about migrating data in and out of the AWS services, see Migration & Transfer on AWS.</p>

OM-2.5.2 Outsourcing Arrangements (Continued)

CBB Rulebook Section - OM - 2.5.2	
Requirement	Considerations
<p>For the purposes of Paragraph OM-2.5.1(c)1 above, Licensees as part of their assessments may use options including:</p> <p>a) Independent third-party certifications on the outsourcing service provider's security and other controls; and</p> <p>b) Third-party or internal audit reports of the outsourcing service provider.</p>	<p>Shared Responsibility</p> <p>AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. AWS will implement and maintain an information and security program which is designed to provide at least the same level of protection as evidenced by:</p> <ul style="list-style-type: none"> the AWS security controls verified by AWS' appropriately skilled and knowledgeable external auditors in its then current System Organization Controls 1, Type 2 report ("SOC 1 Report") and its then current System Organization Controls 2, Type 2 report (for availability/security and confidentiality) ("SOC 2 Report", together with the SOC 1 Report, the "Reports"; its then current certification under ISO 27001; and its then current status as a Level 1 service provider under PCI DSS (together with the ISO 27001, the "Certifications") <p>or, in each case, such alternative industry standard reports or certifications that are its successor or reasonable alternative (provided that they are at least as protective as the standards set out above) as determined by AWS (collectively, the "Certification Standards") which will be AWS's Confidential Information.</p> <p>Customer may, at no additional charge, directly access and download copies of AWS' SOC 1 Report, SOC 2 Report, ISO 27001 and PCI DSS certifications through the AWS Site (as at the Effective Date, located at https://aws.amazon.com/artifact/) ("AWS Artifact"). In the event that AWS no longer maintains such website, provided that Customer and AWS have a valid and applicable NDA in place, Customer may request copies of AWS' security and compliance reports directly from AWS. For the avoidance of doubt, it will not constitute a breach of AWS's obligations pursuant to this Section if exceptions are identified in any SOC 1 Report or SOC 2 Report (or their successor or alternatives), provided that AWS has taken appropriate steps, in its sole discretion, to remediate those exceptions.</p>

OM-2.6 Contingency Planning for Outsourcing Arrangements

CBB Rulebook Section - OM – 2.6	
	Considerations

Requirement	
<p>Licensees must maintain and regularly review contingency plans to enable them to set up alternative arrangements, with minimum disruption to business, should the outsourcing contract be suddenly terminated or the outsourcing service provider fails. This may involve the identification of alternative outsourcing service providers or the provision of the service in-house.</p> <p>These plans must consider how long the transition would take and what interim arrangements would apply.</p>	<p>Shared Responsibility</p> <p>AWS provides Licensee with the capability to implement a robust continuity plan, including frequent server instance backups, 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 disaster recovery approaches, see Disaster Recovery.</p> <p>AWS customers can leverage the features of the AWS infrastructure and AWS services to meet a wide range of resiliency goals. Using multiple Availability Zones, even within a single Region, can enhance resiliency as compared to an on-premises environment. Availability Zones are designed to mitigate against the risk of natural disaster and other disruptions that may occur. Availability Zones are physically separated within a metropolitan region and are in different flood plains. Each Availability Zone is also designed as an independent failure zone and automated processes move customer traffic away from the affected area in the case of failure.</p> <p>Customers can achieve extremely high recovery time and recovery point objectives by using multiple Availability Zones and data replication.</p> <p>Licensees should consider the relevant restrictions on any overseas storage personal data in any contingency plans and any consent requirements under the PDPL. See the additional information provided and referred to at Section OM - 2.5.1.b above.</p>

OM-2.8 Outsourcing of Functions Containing Customer Information

CBB Rulebook Section - OM - 2.8.1		Well-Architected framework considerations
Requirement	Considerations	
<p>Licensees must seek the CBB's prior written approval for third party and intragroup outsourcing of functions/services containing customer information including</p>	<p>Customer Responsibility</p> <p>It is the Licensee's responsibility to seek the CBB's prior written approval for third party and intragroup outsourcing containing customer information.</p>	<p>SEC-9 Protect data in transit</p> <p>REL-9 Secure and encrypt backups</p>

but not limited to payment services, debt collection, card and data processing, IT function including cloud services, internal audit and electronic/internet banking services but excluding legal services. Customer information must be encrypted and the encryption keys or similar forms of authentication codes must be securely kept under the Licensee's control.

For considerations about encryption of customer information, see our comments to requirement **OM-2.8.6**

Requirement		Well-Architected framework considerations
CBB Rulebook Section - OM - 2.8.4	Considerations	
<p>In case of an outsourcing arrangement that involves disclosure of confidential information to the outsourcing service provider, Licensees must ensure that the contract with the outsourcing service provider clearly requires the latter to safeguard the confidentiality of the confidential information; provided always that the responsibility for disclosure of such confidential information must rest with the Licensee. Due consideration must also be given to Law No. 30 of 2018, Personal Data Protection Law</p>	<p>Shared Responsibility</p> <p>For considerations about customer data confidentiality see our comments to requirement OM-2.5.1.b</p>	<p>Not applicable.</p>

(PDPL) issued on 12 July 2018
and the CBB Law.

Cloud Services

For the purpose of outsourcing of cloud services, Licensees must ensure that, at a minimum, the following security measures are in place and included in the outsourcing agreement:

CBB Rulebook Section - OM - 2.8.6		Well-Architected framework considerations
Requirement	Considerations	
1. Customer information must be encrypted and Licensees must ensure that all encryption keys or similar forms of authentication are kept secure and under the Licensee's control.	<p>Customer Responsibility</p> <p>Customers manage access to their customer content and AWS services and resources.</p> <p>We offer our customers strong encryption for customer content in transit or at rest, and we provide customers with the option to manage their own encryption keys.</p> <p>AWS Key Management Service (AWS KMS) allows customers to create and manage cryptographic keys and control their use across a wide range of AWS services and in their applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect customer keys. AWS KMS is integrated with AWS CloudTrail, to provide logs of all key usage.</p> <p>Customer Master Keys (CMKs) used for cryptographic operations in AWS KMS, including operations by AWS employees, are secured by both technical and operational controls. By design, no individual AWS employee can gain access to the physical CMK material in the service due to hardening techniques such as never storing plaintext master keys on persistent disk, using but not persisting them in volatile memory, and limiting which users and systems can connect to service hosts. In addition, multi-party access controls are enforced for</p>	<p>SEC-8 Protect data at rest</p> <p>SEC-9 Protect data in transit</p>

operations on the KMS-hardened security appliances that handle plaintext CMKs in memory.

AWS enables customers to open a secure, encrypted session to AWS servers using HTTPS (Transport Layer Security [TLS]). Additionally, AWS offers customers the ability to add an additional layer of security to data at rest in the cloud, providing scalable and efficient encryption features. It is the responsibility of the AWS customer to enable these features for their systems.

These features include:

- Data encryption capabilities available in AWS storage and database services, such as [Amazon EBS](#), [Amazon S3](#), [Amazon Glacier](#), [Amazon RDS for Oracle](#), [Amazon RDS for SQL Server](#), and [Amazon Redshift](#).
- Flexible key management options, including [KMS](#), allow customers to choose whether to have AWS manage the encryption keys or enable customers to keep complete control over their keys.
- AWS customers can employ Server Side Encryption (SSE) with [Amazon S3](#)-Managed Keys (SSE-S3), SSE with AWS KMS-Managed Keys (SSE-KMS), or SSE with customer-provided keys (SSE-C).

For more information, see [Protecting Data Using Server-Side Encryption](#).

2. Secure audit trail must be maintained for all actions performed by the cloud service provider

Shared Responsibility

AWS offers numerous services to customers to enable them to track, monitor, analyze, and audit events.

[AWS CloudTrail](#) – Enables governance, compliance, operational auditing, and risk auditing of your AWS account. With [AWS CloudTrail](#), you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. [AWS CloudTrail](#) provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

[AWS Config](#) enables customers to continuously monitor and record their AWS resource configurations, and automatically evaluate the

[SEC-2](#) Manage identities for people and machines

[SEC-4](#) Detect and investigate security events

recorded configurations against the desired configurations. [Amazon CloudWatch](#) allows customers to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. Customers can use [Amazon CloudWatch](#) to gain system-wide visibility into resource utilization, application performance, and operational health.

AWS provides up-to-the-minute information on the health of AWS services at the publicly available Service Health Dashboard. Customers can configure a Personal Health Dashboard to receive a personalized view of the performance and availability of the AWS services underlying their resources and applications. The dashboard displays relevant and timely information to help customers manage events in progress, and it provides proactive notification to help customers plan for scheduled activities. With Personal Health Dashboard, changes in the health of AWS resources automatically trigger alerts, providing event visibility and guidance to help quickly diagnose and resolve issues. Customers can use these insights to react and keep their applications running smoothly.

[Amazon Virtual Private Cloud](#) (Amazon VPC) Flow Logs – VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to [Amazon CloudWatch](#) Logs and [Amazon S3](#). After you've created a flow log, you can retrieve and view its data in the chosen destination.

[Amazon S3](#) Server Access Logging – Server access logging provides detailed records for the requests that are made to a bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits.

3. Comprehensive change management procedure must be developed to account for future changes in technology with adequate testing of such changes.

Shared Responsibility

AWS has established and maintains company-wide policy that defines roles, responsibilities and classifications for managing changes to the production environment. Changes to AWS services and features follow secure software development practices, which include a security risk review prior to launch.

[SEC-6](#) protect compute resources

AWS developers that require access to production environments must explicitly request access through the AWS access management system, have the access reviewed and approved by the appropriate owner, and upon approval obtain authentication. AWS service teams maintain service specific change management standards that inherit and build on the AWS Change Management guidelines.

AWS applies a systematic approach to managing change to ensure that all changes to a production environment are reviewed, tested, and approved. The AWS Change Management approach requires that the following steps be complete before a change is deployed to the production environment:

1. Document and communicate the change via the appropriate AWS change management tool.
2. Plan implementation of the change and rollback procedures to minimize disruption.
3. Test the change in a logically segregated, non-production environment.
4. Complete a peer-review of the change with a focus on business impact and technical rigor. The review should include a code review.
5. Attain approval for the change by an authorized individual.

Where appropriate, a continuous deployment methodology is conducted to ensure changes are automatically built, tested, and pushed to production, with the goal of eliminating as many manual steps as possible. Continuous deployment seeks to eliminate the manual nature of this process and automate each step, allowing service teams to standardize the process and increase the efficiency with which they deploy code. In continuous deployment, an entire release process is a "pipeline" containing "stages".

AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet.

All changes to the AWS production environment are reviewed on at least a monthly. An audit trail of the changes is maintained for a least a year.

Emergency changes follow the AWS incident response procedures. Exceptions to the change management processes are documented and escalated to AWS management.

4. The Licensee's data must be logically segregated from data of other entities at the cloud service provider's platform; and

Shared Responsibility

SEC-1 Operate workload securely

The [Logical Separation Handbook](#) will help Licensees understand logical separation in the cloud and demonstrates its advantages over a traditional physical separation model.

Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Licensees maintain full control over who has access to their data. AWS services which provide virtualized operational environments to customers (i.e., EC2) ensure that customers are segregated from one another and prevent cross-tenant privilege escalation and information disclosure via hypervisors and instance isolation.

Different instances running on the same physical machine are isolated from each other via the hypervisor. In addition, the Amazon EC2 firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer; thus, an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical random-access memory (RAM) is separated using similar mechanisms.

Customer instances have no access to physical disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically erases every block of storage before making it available for use, which protects one customer's data from being unintentionally exposed to another. Customers can further protect their data using traditional filesystem encryption mechanisms, or, in the case of [Amazon Elastic Block Store](#) (Amazon EBS) volumes, by enabling AWS-managed disk encryption.

A Dedicated Host is also a physical server that's dedicated for customer use. With a Dedicated Host, customers have visibility and control over how hypervised instances are placed on the server. Bare

metal instances are non-hypervised host hardware devices. Using the [AWS Nitro](#) technology for network and storage offload, as well as the Nitro security chip to eliminate the risks associated with serial single-tenancy on bare metal, customers have direct access to Amazon EC2 hardware. These bare metal instances are full-fledged members of the Amazon EC2 service and have access to AWS services such as [Amazon VPC](#) and [Amazon Elastic Block Store \(EBS\)](#).

5. The cloud service provider must have in place measures to ensure adequate information / data security, data security and confidentiality, including but not limited to forms of protection available against unauthorized access and incident management process in cases of data breach or loss; and

Shared Responsibility

AWS has established an information security management program with designated roles and responsibilities that are appropriately aligned within the organization. AWS management reviews and evaluates the risks identified in the risk management program at least annually. The risk management program encompasses the following phases:

- a. **Discovery** – The discovery phase includes listing out risks (threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- b. **Research** – The research phase considers the potential impact(s) of identified risks to the business and its likelihood of occurrence and includes an evaluation of internal control effectiveness.
- c. **Evaluate** – The evaluate phase includes ensuring controls, processes and other physical and virtual safeguards are in place to prevent and detect identified and assessed risks.
- d. **Resolve** – The resolve phase results in risk reports provided to managers with the data they need to make effective business decisions and to comply with internal policies and applicable regulations.
- e. **Monitor** – The monitor phase includes performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed.

Reports and certifications available to customers on demand.

SEC-10 Develop incident management plans

6. Any disclosure of customer information by the cloud service provider to a foreign court, government or law enforcement agency or to any third party must be in compliance with all legal and regulatory requirements in the Kingdom of Bahrain. Procedures to be followed in such instances must be clearly stipulated in the outsourcing agreement including the requirement to notify the licensee of the request and the response of the cloud service provider to such request.

Shared Responsibility

Amazon does not disclose customer information in response to government demands unless we're required to do so to comply with a legally valid and binding order. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing content information.

Where we need to act to protect customers, we do. We have repeatedly challenged government demands for customer information that we believed were overbroad, winning decisions that have helped to set the legal standards for protecting customer speech and privacy interests. We also advocate in Congress to modernize outdated privacy laws to require law enforcement to obtain a search warrant from a court to get the content of customer communications. That's the appropriate standard, and it's the standard we follow.

For AWS clients, we offer strong encryption as one of many standard security features, and we provide them the option to manage their own encryption keys. We publish security best practices documents on our website and encourage our clients to use these measures to protect sensitive content. Content that has been encrypted is rendered useless without the applicable decryption keys.

We are members of numerous associations focused on protecting privacy and security, and AWS in particular has achieved a number of internationally recognized certifications and accreditations demonstrating compliance with third-party assurance frameworks. AWS clients have control over their content and where it resides.

[SEC-8](#) Protect data at rest

[SEC-9](#) Protect data in transit

[REL-9](#) Secure and encrypt backups

The licensee must obtain information from the cloud service provider on all the measures mentioned in Paragraph OM-2.8.6 to ensure compliance, prior to

Shared Responsibility

The AWS [Law Enforcement Information Request page](#) will help customers to ensure their compliance with Paragraph OM-2.8.6 prior to commencing outsourcing to the cloud service provider.

commencing outsourcing to the cloud service provider.

Requirement – OM 2.8.7	Considerations
<p>The Licensees should consider how the variety of risks associated with the cloud adoption illustrated below are managed:</p> <ul style="list-style-type: none"> a. Vendor lock-in (cloud vendor using proprietary technology preventing migration); 	<div data-bbox="602 632 862 663">Shared Responsibility</div> <p>Customers retain control and ownership of their data. The use of AWS cloud services does not give rise to a risk of lock-in, as customers have complete flexibility to port their data between interoperable services offered by AWS and others, for the following reasons.</p> <div data-bbox="602 940 1333 1310">No long-term commitments – Customers are able to adopt the cloud on their own terms. AWS is designed such that customers only use the services that they wish to use alongside the technology of their own choice. As AWS offers pay-as-you-go pricing, customers have the ability to shut down their environment, export their data and virtual machines, and migrate at their own discretion. AWS enables customers to move data as needed on and off AWS storage. AWS support plans function similarly and are billed monthly without any long-term commitments or contracts, regardless of tier.</div> <div data-bbox="602 1350 1333 1591">Tools and services built to support portability – AWS cloud services are built to support migration into and out of AWS, and this is easily enabled by the tools and techniques offered by AWS. For example, AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS, using portable storage devices for transport.</div> <div data-bbox="602 1631 1333 1829">Open standards and interoperable solutions – AWS Cloud services are built on numerous open standards such as SQL, Linux, and Xen. This flexible foundation allows customers to securely move information in and out of the cloud, regardless of where that information is going: cloud-to-cloud or cloud-to-data center.</div> <div data-bbox="1344 632 1555 856"> <p>OPS-1 Determine priorities</p> <p>COST-5 Evaluate cost when selecting services</p> </div>

Requirement – OM 2.8.7	Considerations
<p>b. Vendor lock-out (cloud going out of business, preventing access to data);</p>	<p>Shared Responsibility</p> <p>The use of AWS cloud services does not give rise to a risk of lock-out, as customers will remain in control and possession of their data, for the following reasons.</p> <p>Customer control over data – Customers retain control and ownership of their data and AWS enables customers to move data on and off AWS storage (as needed).</p> <p>Simultaneous use of alternative back-up options – AWS enables customers to perform their own backups through AWS Backup. Customers can centrally manage and automate backups across AWS cloud services. Easily and quickly, customers are able to create backup policies that automate backup schedules and retention management. Simultaneous use of alternative storage options – AWS also offers the Storage Gateway, a hybrid cloud storage service which allows customers to mix cloud storage with on-premises applications and storage. Customers can use it as network file storage, or for backup (or both). Since it can be integrated with customers' local networks (and because data transfer is two-way), this service enables customers to use AWS cloud storage, while at the same time maintaining or mirroring important data locally. In turn, this means that, even in the highly unlikely event of AWS going out of business, customers have the option of being able to access their data locally.</p>

[SEC-8](#) Protect data at rest

[SEC-9](#) Protect data in transit

[REL-9](#) Secure and encrypt backups

[PERF-3](#) Storage Solution

Requirement – OM 2.8.7	Considerations
<p>c. Data and application interoperability;</p>	<p>Shared Responsibility</p> <p>AWS products and services facilitate interoperability with third party services. AWS cloud services are built on numerous open standards such as SQL, Linux, and Xen. This flexible foundation allows customers to securely move information in and out of the cloud, regardless of where that information is going: cloud-to-cloud or cloud-to-data center. AWS provides a number of migration tools to not only allow customers to easily move resources from on-premises to AWS, but also move resources back on-premises if customers so choose. For example, AWS Server Migration Service, allows customers to migrate thousands of on-premises workloads to AWS and to automate, schedule and track incremental replications of live server volumes, making it easier for customers to coordinate large-scale server migrations. In addition, AWS Database Migration Service supports both homogeneous and heterogeneous migrations between different database platforms. The wide range of migrations can be easily tracked by the customer on the AWS Migration Hub which provides a central location for discovering, planning and tracking data migration.</p> <p>SEC-8 Protect data at rest</p> <p>SEC-9 Protect data in transit</p> <p>REL-9 Secure and encrypt backups</p> <p>PERF-3 storage solution</p>

Requirement – OM 2.8.7	Considerations
d. Segregation of data in SaaS environments;	<p data-bbox="605 352 889 384">Customer Responsibility</p> <p data-bbox="605 422 1333 917">Security and compliance is a shared responsibility between AWS and the customer. AWS is responsible for the security and compliance 'of' the cloud, and implements security controls to secure the underlying infrastructure that runs the AWS services and hosts and connects customer resources. AWS customers are responsible for security 'in' the cloud and should determine, design and implement the security controls needed based on their security and compliance needs and AWS services they select. The customer responsibility will be determined by the AWS services that a customer selects. AWS provides customers with best practices on how to secure their resources within the AWS service's documentation at http://docs.aws.amazon.com/.</p> <p data-bbox="1362 352 1555 426">SEC-1 Operate workload securely</p>

e. Distributed denial of service (DDoS) prevention;
Shared Responsibility

The AWS Network consists of the internal data center facilities, servers, networking equipment and host software systems that are within AWS' control and are used to provide the services.

SEC-5 Protecting network resources

SEC-6 Protect compute resources

The AWS network provides significant protection against traditional network security issues. For example:

REL-11 Design workload to withstand component failures

- Distributed Denial of Service (DDoS) Attacks. AWS API endpoints are hosted on large, Internet-scale infrastructure and use proprietary DDoS mitigation techniques. Additionally, AWS' networks are multi-homed across a number of providers to achieve Internet access diversity.

REL-3 Design workload service architecture

- Man in the Middle (MITM) Attacks. All of the AWS APIs are available via TLS/SSL-protected endpoints, which provide server authentication. Amazon EC2 AMIs automatically generates new SSH host certificates on first boot and logs them to the instance's console. Customers can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. Customers can use TLS/SSL for all of their interactions with AWS.

- IP Spoofing. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

- Port Scanning. Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. Customers can report suspected abuse using the contacts available on our website at: <http://aws.amazon.com/contact-us/report-abuse/>. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by the customer. Customers' strict management of security groups can further mitigate the threat of port scans. Customers may request permission

Requirement – OM 2.8.7**Considerations**

to conduct vulnerability scans as required to meet specific compliance requirements. These scans must be limited to customers' own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans can be initiated by submitting a request via the website at:

<http://aws.amazon.com/security/penetration-testing/>.

- Packet sniffing by other tenants. Virtual instances are designed to prevent other instances running in promiscuous mode to receive or “sniff” traffic that is intended for a different virtual instance. While customers can place interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other's traffic. While Amazon EC2 does provide protection against one customer inadvertently or maliciously attempting to view another's data, as a standard practice customer can encrypt sensitive traffic.

In addition, firewall devices are configured to restrict access to Amazon's corporate and production networks. The configurations of these firewall policies are maintained using an automatic push from a parent server every 24 hours. All changes to the firewall policies are reviewed and approved.

Network devices, including firewall and other system boundary devices are configured to fail securely in the event of an operational failure. Boundary firewalls and load balancer devices are set to fail to deny all until the device's functionality is restored.

Requirement – OM 2.8.7	Considerations
f. Impact of regulatory enforcement processes;	<p>Shared Responsibility</p> <p>Compliance is a shared responsibility between AWS and the Customer.</p> <p>AWS documents, tracks and monitors its legal, regulatory and contractual agreements and obligations.</p> <p>AWS maintains relationships with internal and external parties to monitor legal, regulatory, and contractual requirements. Should a new directive be issued, AWS creates and documents plans to implement the directive within a designated timeframe.</p> <p>AWS provides Customers with evidence of its compliance with applicable legal, regulatory, and contractual requirements through audit reports, attestations, certifications and other compliance enablers. Visit aws.amazon.com/artifact for information on how to review the AWS external attestation and assurance documentation.</p> <p>AWS Customers remain responsible for their own compliance with regulatory enforcement processes impacting their adoption and use of AWS services. AWS provides customers with best practices on how to secure their resources and ensure compliance within the AWS service's documentation at http://docs.aws.amazon.com/.</p>

OPS-1 Determine priorities

SEC-1 Operate workload securely

g. Safeguards for management of cryptographic keys;
Shared Responsibility
[SEC-8](#) Protect data at rest

AWS is designed to protect the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help ensure that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected. AWS provides several methods for customers to securely handle their data:

[SEC-9](#) Protect data in transit

-Upon initial communication with an AWS-provided Windows Amazon Machine Image (AMI), AWS enables secure communication by configuring terminal services on the instance and generating a unique self-signed X.509 server certificate and delivering the certificate's thumbprint to the user over a trusted channel.

-AWS further enables secure communication with Linux AMIs by configuring Secure Shell (SSH) on the instance, generating a unique host-key and delivering the key's fingerprint to the user over a trusted channel.

Customer Master Keys (CMKs) used for cryptographic operations in AWS Key Management Service (KMS), including operations by AWS employees, are secured by both technical and operational controls. By design, no individual AWS employee can gain access to the physical CMK material in the service due to hardening techniques such as never storing plaintext master keys on persistent disk, using but not persisting them in volatile memory, and limiting which users and systems can connect to service hosts. In addition, multi-party access controls are enforced for operations on the KMS-hardened security appliances that handle plaintext CMKs in memory.

AWS enables customers to open a secure, encrypted session to AWS servers using HTTPS (Transport Layer Security [TLS]). Additionally, AWS offers customers the ability to add an additional layer of security to data at rest in the cloud, providing scalable and efficient encryption features. It is the responsibility of the AWS customer to enable these features for their systems.

Requirement – OM 2.8.7	Considerations
	<p>These features include:</p> <ul style="list-style-type: none">-Data encryption capabilities available in AWS storage and database services, such as Amazon EBS, Amazon S3, Amazon Glacier, Amazon RDS for Oracle, Amazon RDS for SQL Server, and Amazon Redshift.-Flexible key management options, including KMS, allow customers to choose whether to have AWS manage the encryption keys or enable customers to keep complete control over their keys.-AWS customers can employ Server Side Encryption (SSE) with Amazon S3-Managed Keys (SSE-S3), SSE with AWS KMS-Managed Keys (SSE-KMS), or SSE with customer-provided keys (SSE-C). <p>For more information, visit http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html.</p>

Requirement – OM 2.8.7	Considerations
<p>h. Unmonitored access to administrative zones by staff and 3rd parties;</p>	<p>Shared Responsibility</p> <p>Amazon personnel with a business need to access the management plane are required to first use multi-factor authentication, distinct from their normal corporate Amazon credentials, to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked.</p> <p>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 utilizing some form of multi-factor authentication to gain access to customer instances (or at a minimum key-based SSH Version 2 access). Amazon-provided images, Amazon Machine Images (AMI), default to only allowing the key pair specified by API call at the time of instance creation to be able to access the instance, or to decrypt the randomly generated administrator password for Windows instances. Additionally, customers can employ a privilege escalation mechanism with logging on a per-user basis. For example, if the guest OS is Linux, after hardening an instance, customers can utilize key-based SSHv2 to access the virtual instance, disable remote root login, use command-line logging, and use 'sudo' for privilege escalation. Customers can generate their own key pairs in order to guarantee that they are unique, and not shared with other customers or with AWS.</p> <p>SEC-2 Manage identities for people and machines</p> <p>SEC-3 Manage permissions for people and machines</p> <p>SEC-4 Detect and investigate security events</p>

i. Remote access to administrative zones without strong authentication and accountability;

Shared Responsibility

Security and compliance is a shared responsibility between AWS and the Customer.

AWS requires multi-factor authentication over an approved cryptographic channel when accessing the AWS production environment remotely.

Remote access to AWS production environments is limited to defined security groups. The addition of members into a group must be reviewed and approved by authorized individuals who confirm the user's need for access to the environment. Baselining of groups (e.g., reviewing of existing members in the group for their continued need for access) occurs every 90 days by the manager and is enforced by the permissions tool which provides automated notification to the manager.

AWS employs automated mechanisms to facilitate the monitoring and control of remote access methods. Auditing occurs on the systems and devices, which are then aggregated and stored in a proprietary tool for review and incident investigation. The AWS operational environment, to include network and security configuration, is considered confidential information and is required to be protected by employees per Amazon data classification policies.

AWS does not allow collaborative computing devices to connect to the production systems that process or store customer data

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 utilizing some form of multi-factor authentication to gain access to customer instances (or at a minimum key-based SSH Version 2 access). Amazon-provided images, Amazon Machine Images (AMI), default to only allowing the key pair specified by API call at the time of instance creation to be able to access the instance, or to decrypt the randomly generated administrator password for Windows instances.

[SEC-2](#) Manage identities for people and machines

[SEC-3](#) Manage permissions for people and machines

[SEC-4](#) Detect and investigate security events

Requirement – OM 2.8.7	Considerations
<p>j. Single point of failures in connectivity to cloud environments</p>	<p>Share Responsibility</p> <p>Amazon’s infrastructure has a high level of availability and provides you with the capability to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.</p> <p>Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is “cold.” In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.</p> <p>AWS provides you 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 utilizing discrete uninterruptable power supply (UPS) and onsite backup generators, they are each fed via 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> <p>You should architect your AWS usage to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure scenarios, including natural disasters or system failures. However, you should be aware of location-dependent privacy and compliance requirements, such as the EU Data Privacy Directive. Data is not replicated between regions unless proactively done so by the customer, thus allowing customers with these types of data placement and privacy requirements the ability to establish compliant environments. It should be noted that all communications between regions is across public internet infrastructure; therefore, appropriate encryption methods should be used to protect sensitive data.</p> <p>OPS-4 Understand workload state</p> <p>SEC-5 Protecting network resources</p> <p>REL-2 Plan network topology</p> <p>PERF-5 Configure networking solution</p>

CBB Rulebook Section - OM - 2.8.8	
Requirement	Considerations
The Licensees must ensure that outsourcing to cloud service providers does not result in data being stored in countries that are subject to United Nations sanctions.	<p>Shared Responsibility</p> <p>AWS customers designate in which geographic region their customer content will be stored. We will not move or replicate customer content outside of the customer's chosen region(s), except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users</p> <p>Licensees should also consider the relevant restrictions on any overseas storage personal data in any contingency plans and any consent requirements under the PDPL. See the additional information provided and referred to at Section OM - 2.5.1.b above.</p>

Appendix 2: Due Diligence components

Licensee Board of directors and senior management should establish a comprehensive and ongoing due diligence **and oversight process for managing Licensee's outsourcing relationships**. Below some due diligence components:

Financial soundness: **AWS is an industry leader in a large and rapidly growing market segment. AWS has an annual revenue run rate in the tens of billions of U.S. dollars, with consistent double-digit year-on-year revenue growth and significant operating margins and profits. Further, AWS is wholly-owned by Amazon.com, Inc., one of the top 20 companies globally by revenue.** The financial statements of Amazon.com Inc. include AWS's sales and income, permitting assessment of its financial position and ability to service its debts and/or liabilities. These financial statements are available from the SEC or at Amazon's Investor Relations website.

Reputation: 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, allowing us to provide

new services that help millions of active customers. **AWS is the world's most comprehensive and broadly adopted cloud platform, offering over 165 fully featured services from data centers globally.**

Managerial skills: 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.

Technical capabilities, operational capability and capacity: The AWS Cloud operates a global infrastructure with multiple Availability Zones within multiple geographic AWS Regions around the world. For more information, see AWS Global Infrastructure. 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 data. Maintaining customer trust and confidence is of the utmost importance to AWS. 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.

Compatibility with the Licensee's corporate culture and future development strategies: AWS maintains a systematic approach to planning and developing new services for the AWS environment to ensure that the quality and security requirements are met with each release. The AWS strategy for the design and development of AWS services is to clearly define AWS services in terms of customer use cases, service performance, marketing and distribution requirements, production and testing, and legal and regulatory requirements.

Familiarity with the banking industry and capacity to keep pace with innovation in the market: For a list of case studies from financial services customers that have deployed applications on the AWS Cloud, see Financial Services Customer Stories. For a list of financial services solutions provided by AWS, see Financial Services Cloud Solutions.