AWS User Guide for Federally Regulated Financial Institutions in Canada

March 2024

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 Amazon Web Services (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.

Contents

Abstract

This guide provides information to assist federally regulated financial institutions in Canada as they accelerate their use of Amazon Web Services (AWS) cloud services.

This guide:

- Describes the respective roles that the customer and AWS each play in managing and securing the cloud environment
- Describes AWS security systems and shared responsibility model
- Provides an overview of regulatory requirements and guidance applicable to the use of AWS cloud services
- Provides additional resources to assist customers to design and architect their AWS environment to meet their security and regulatory objectives

Introduction

Around the world, financial institutions (FIs) use Amazon Web Services (AWS) to modernize and automate their core applications, including mobile banking, regulatory reporting, and market analysis. Through continuous innovation, AWS provides strong security systems, a broad and deep set of services and features, deep industry expertise, and an expansive partner network available to FIs globally. AWS empowers FIs to modernize their technology infrastructure, meet rapidly changing customer behaviors and expectations, and drive business growth. AWS offers IT services in categories ranging from compute, storage, database, and networking to artificial intelligence and machine learning.

The Office of the Superintendent of Financial Institutions (OSFI) is the prudential regulator of federally regulated financial institutions (FRFIs) and certain private pension plans in Canada. FRFIs include all banks and federally incorporated or registered trust and loan companies, as well as certain insurance companies, cooperative credit associations, and fraternal benefit societies in Canada.

OSFI publishes Guidelines, which reflect OSFI's expectations of FRFIs with respect to management of non-financial risks (for example, operational risk). The Guidelines set standards that govern industry activities and behavior, including sound business and financial practices.

This guide is intended to be a resource to help FRFIs understand certain key technical and operational requirements for the use of AWS services in Canada. This guide includes a description of the advanced tools and security measures offered by AWS that FRFIs can use to assist them with evaluating, meeting, and demonstrating compliance with regulatory requirements outlined in applicable OSFI Guidelines.

This guide doesn't undertake a full analysis of OSFI Guidelines; rather, the sections listed below provide information on AWS services, features, and resources that might help FRFIs address certain OSFI expectations for sound risk management.

- **Security and shared responsibility**: It's important that FRFIs understand the AWS Shared Responsibility Model before evaluating the specific technical and operational requirements outlined in OSFI's Guidelines. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS for security and informs the steps FRFIs should take as they look to comply with the relevant requirements.

- **AWS Compliance Programs and AWS Compliance Center**: AWS has obtained certifications and third-party attestations for a variety of industry-specific and general workloads. AWS has also developed compliance programs to make these resources available to customers. Customers can take advantage of AWS Compliance Programs to help satisfy their regulatory requirements.

  The AWS Compliance Center is a central location to research cloud-related regulatory requirements and how they impact your industry. Select the country you are interested in, and the AWS Compliance Center will display the country's regulatory position regarding the adoption of cloud services.

- **AWS Global Cloud Infrastructure**: The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones. The AWS Global Cloud Infrastructure offers AWS customers an easier and more effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than traditional on-premises environments. AWS customers can use the AWS Global Cloud Infrastructure to help them design an AWS environment consistent with their business and regulatory needs.

- **Considerations for federally regulated financial institutions**: This section provides an overview of the key technical and operational requirements for FRFIs that are seeking to use AWS services. A more detailed list of requirements and corresponding considerations is provided in the Appendix, which describes how FRFIs can use various AWS services, features, tools, and resources to help them comply with certain regulatory requirements.

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

This document is provided for informational purposes only; it is not legal or compliance advice and should not be relied on as legal or compliance advice. Customers are responsible for making their own independent assessments and should obtain appropriate advice from their own legal and compliance advisors regarding compliance with applicable Canadian laws and regulations, including OSFI Guidelines.

Security and the AWS Shared Responsibility Model

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 programs that they choose to implement to protect their content, applications, systems, and networks, no differently than they would for applications in an on-premises data center.

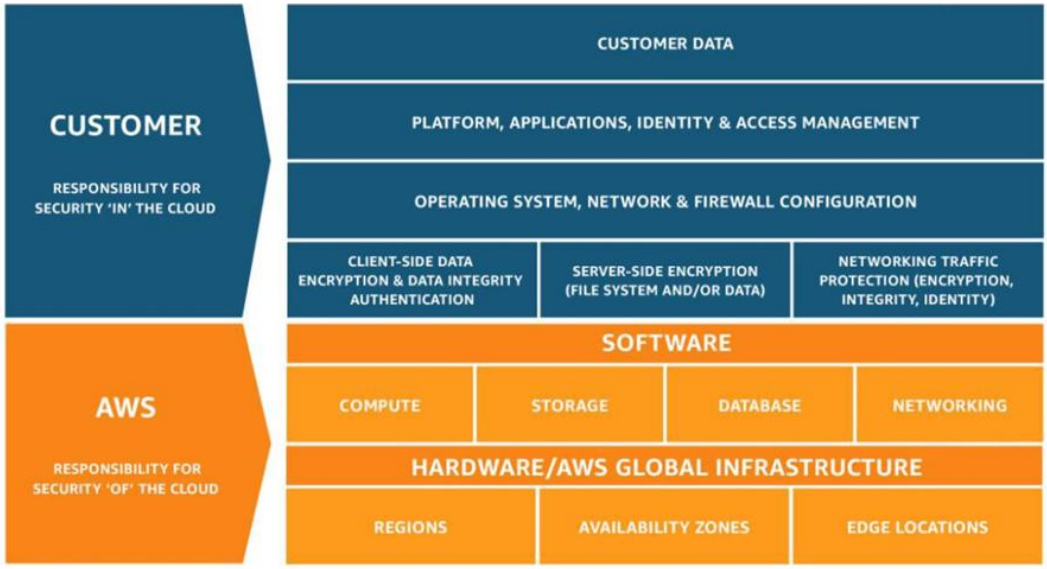

Figure 1: AWS Shared Responsibility Model

The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of cloud security principles. AWS operates, manages, and controls the IT components, from the host operating system and virtualization layer down to the physical security of the facilities where the services operate. For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and environments, and customers access the endpoints to store and retrieve data.

Security in the cloud

Customers are responsible for their security in the cloud. Customer responsibility is determined by the AWS Cloud services that a customer selects. The services selected determine 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 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 security groups. A security group acts as a firewall that controls the traffic allowed to and from the resources in a virtual private cloud (VPC). Customers can choose the ports and protocols to allow for inbound traffic and for outbound traffic. For each security group, customers add separate sets of rules for inbound traffic and outbound traffic.

For abstracted services, such as Amazon S3 and DynamoDB, AWS operates the infrastructure layer, the operating system, and environments, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using AWS Identity and Access Management (IAM) tools to apply the appropriate permissions. Therefore, customers should carefully consider the services they choose because their responsibilities will vary depending on the services they use, the integration of those 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 and Region where they store their content
- The format and structure of their content and whether it is masked, anonymized, or encrypted
- How their data is encrypted, and where the keys are stored
- Who has access to their content and how those access rights are granted, managed, and revoked

Security of the cloud

AWS regularly achieves third-party validation for thousands of global compliance requirements that we continually monitor to help customers meet their security and compliance standards. Customers can use compliance certifications earned by AWS to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications. In support of our compliance program, AWS undertakes the following actions:

- **Validate** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that customers can implement and to better assist customers with managing their control environment.
- **Demonstrate** the AWS compliance posture to help customers verify their 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 in turn use this information to perform their control evaluation and verification procedures under the applicable compliance standard.
- **Monitor**, through applicable security controls, that AWS maintains compliance with global standards and best practices.

AWS compliance programs

AWS 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. Customers can use 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 might be of particular importance to FRFIs:

- **CCCS** – The Canadian Centre for Cyber Security (CCCS) is Canada's authoritative source of cyber security expert guidance for Canadian government, industry, and the general public. Public and commercial sector organizations across Canada rely on the CCCS Cloud service provider (CSP) information technology security (ITS) assessment process in their decision to use AWS. CCCS's assessment process determines if the Government of Canada (GC) ITS requirements for the CCCS Medium Cloud Security Profile (previously referred to as GC's PROTECTED B/Medium Integrity/Medium Availability [PBMM] profile) are met as described in ITSG-33 (IT Security Risk Management: A Lifecycle Approach, Annex 3 – Security Control Catalogue). As of November 2023, 150 services and features have been assessed by the CCCS and meet the requirements for Medium Cloud Security Profile. For more information, see the CCCS Assessment webpage.

- **ISO 27001** – ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls that follow the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an information security management system which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.

- **ISO 27017** – ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional implementation guidance for information security controls specific to cloud service providers. For more information or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.

- **ISO 27018** – ISO 27018 is a code of practice that focuses on protecting personal data in the cloud. It's based on the ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls that are 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** – ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures that are required to achieve effective quality management within an organization. The key to the ongoing certification under this standard is establishing, maintaining, and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information or to download the AWS ISO 9001 certification, see the ISO 9001 Compliance webpage.

- **PCI DSS Level 1** – The Payment Card Industry Data Security Standard (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) 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. AWS is certified as a PCI DSS Level 1 Service Provider, the highest level of assessment available. 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 Control (SOC) reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls that have been established to support operations and compliance. For more information, see the SOC Compliance webpage. AWS SOC reports come in three forms:

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

    - **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.

See the AWS Compliance Programs webpage for more information about AWS certifications and attestations. See the Best Practices for Security, Identity, & Compliance website for general AWS security controls and service-specific security.

AWS Artifact

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

AWS Global Cloud Infrastructure

The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones. A Region is a physical location in the world that consists 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 that 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 choose the Regions where their content and applications are located. This allows customers to establish environments that meet specific geographic or regulatory requirements. Additionally, this allows customers with business continuity and disaster recovery objectives to establish primary and backup environments in the locations of their choice. More information on our disaster recovery recommendations is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

Considerations for federally regulated financial institutions

- OSFI Guideline No. B-13 outlines OSFI's expectations for the sound management of technology and cyber risk. While there are no requirements specific to cloud services, the outcomes, principles, and expectations apply to all aspects of technology and cyber risk management, including cloud computing.
- OSFI Guideline No. B-10 sets out OSFI's expectations for managing risks associated with third-party arrangements. The guideline applies to all third-party arrangements including cloud services, but OSFI's expectations are scaled based on the assessed level of risk and the criticality of the arrangement to the FRFI's operations. B-10 includes specific expectations for the management of technology and cyber risk in third-party arrangements, as well as expectations specific to cloud adoption.
- OSFI Guideline No. E-21 sets out OSFI's expectations for FRFIs' management of operational risk, defined as "the risk of loss resulting from people, inadequate or failed internal processes and systems, or from external events." While not specific to the use of the cloud, the expectations in this guideline apply to all aspects of a FRFI's operations, including those enabled by cloud services.
- OSFI's advisory on Technology and Cyber Security Incident Reporting governs how FRFIs should disclose and report technology and cyber security incidents to OSFI.
- OSFI also released an updated Cyber Security Self-Assessment that helps FRFIs gauge and improve their current state of readiness with respect to emerging cyber threats. The Cyber Security Self-Assessment examines a FRFI's capability to respond to a cyber incident in areas ranging from organization and resources to how it manages threats, risks, and incidents.

The current version of this guide provides considerations for FRFIs as they assess their responsibilities with regard to OSFI Guideline B-13 – Technology and Cyber Risk Management. Subsequent versions of this guide might be updated to provide considerations for other OSFI guidelines.

Regulations are changing rapidly in this space, and AWS is working to help customers proactively respond to new rules and guidelines. AWS encourages its financial institution customers to obtain appropriate advice on their compliance with all regulatory and legal requirements that are relevant to their business, and local laws, regulations, and guidelines.

OSFI Guideline B-13 – Technology and Cyber Risk Management

Guideline B-13 outlines OSFI's expectations related to technology and cyber risk management and aims to "support FRFIs in developing greater resilience to technology and cyber risks." OSFI states that Guideline B-13 "should be read, and implemented, from a risk-based perspective that allows FRFIs to compete effectively and take full advantage of digital innovation, while maintaining sound technology risk management." OSFI has set an effective date of January 1, 2024, so as to provide FRFIs with sufficient time to self-assess and ensure their compliance with OSFI's expectations for technology and cyber risk management.

Guideline B-13 is organized into three sections or *domains*:

1. **Governance and risk management** – Sets OSFI's expectations for the formal accountability, leadership, organizational structure, and framework used to support risk management and oversight of technology and cyber security.

2. **Technology operations and resilience** – Sets OSFI's expectations for management and oversight of risks related to the design, implementation, management, and recovery of technology assets and services.
3. **Cyber security** – Sets OSFI's expectations for management and oversight of cyber risk.

Each domain has a desired outcome for FRFIs to achieve through managing risks that contribute to developing FRFIs' resilience to technology and cyber risks:

1. Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.
2. A technology environment that is stable, scalable, and resilient. The environment is kept current and supported by robust and sustainable technology operating and recovery processes.
3. A secure technology posture that maintains the confidentiality, integrity, and availability of the FRFI's technology assets.

A full analysis of Guideline B-13 is beyond the scope of this document, however the Appendix addresses considerations in sections 2 and 3 of the Guideline that are most relevant to a FRFI's use of AWS services.

Note: Section 1 of Guideline B-13 sets broad expectations related to technology and cyber governance, strategy, and risk management. As these are customer-specific considerations that aren't directly related to a FRFI's use of AWS services, section 1 has been omitted from this guide.

Getting started

Each organization's cloud adoption journey is unique; therefore, customers need to understand their organization's current state, the desired target state, and the transition required to achieve the target state to complete their cloud adoption successfully. Knowing this will help them set goals and create work streams that will enable their 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 customers 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 learn more about such workshops, customers can contact their 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 FRFIs, next steps typically include the following:

- Contacting an AWS representative to discuss how the AWS Partner Network, and AWS Solution Architects, Professional Services teams, and Training instructors can assist with the cloud adoption journey.
- Obtaining and reviewing a copy of the latest AWS SOC 1 and 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification from AWS Artifact (accessible through the AWS Management Console).

- Considering the relevance and application of the AWS Security Whitepapers, AWS Well-Architected Framework, and the CIS AWS Foundations Benchmark, as appropriate for their 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.
- Diving deeper into other governance and risk management practices as necessary based on their due diligence and risk assessment, using the tools and resources referenced throughout this guide and in the **Additional Resources** section that follows.

In addition to helping our customers maximize the use of the technology provided by AWS, the AWS technical team can support our customers in their efforts to implement architecture, products, and services in compliance with applicable technical and operational requirements.

Support plans

AWS Support plans are designed to give customers the right mix of tools and access to expertise so that they can be successful with AWS while optimizing performance, managing risk, and keeping costs under control.

AWS Basic Support is included for all AWS customers and includes:

- **Customer Service and Communities** – 24/7 access to customer service, documentation, whitepapers, and support forums.
- **AWS Trusted Advisor** – Access to the seven core Trusted Advisor checks and guidance to help customers provision resources following best practices to increase performance and improve security.
- AWS Personal Health Dashboard – A personalized view of the health of AWS services, and alerts when resources are impacted.

Additional resources

- AWS Compliance Quick Reference Guide – AWS has many features to assist you in meeting compliance objectives 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.
- The AWS Security Reference Architecture (AWS SRA) is a holistic set of guidelines for deploying the full complement of AWS security services in a multi-account environment. It can be used to help design, implement, and manage AWS security services so that they align with AWS best practices. The recommendations are built around a single-page architecture that includes AWS security services—how they help achieve security objectives, where they can be best deployed and managed in your AWS accounts, and how they interact with other security services. This overall architectural guidance complements detailed, service-specific recommendations such as those found on the AWS Security website.
- AWS Well-Architected Framework – The Well-Architected Framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures and provides guidance to help implement designs that will scale to meet application needs over time. The Well-Architected Framework consists of six pillars: Operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability.
- AWS has produced whitepapers addressing each pillar of the Well-Architected Framework – AWS Operational Excellence Pillar, AWS Security Pillar, AWS Reliability Pillar, AWS Performance Efficiency Pillar, AWS Cost Optimization Pillar, and AWS Sustainability Pillar.
- The Financial Services Industry Lens of the AWS Well-Architected Framework focuses on designing, deploying, and architecting financial services industry workloads that promote resiliency, security, and operational performance in line with risk and control objectives that FRFIs can define.
- 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 (that is, 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 (that is, security of the cloud). FRFIs can use NIST CSF and AWS resources to elevate their risk management frameworks.

For additional help, visit the Security, Identity, and Compliance Whitepapers.

Appendix: Key considerations for compliance with OSFI Guidelines

This appendix provides suggestions on various AWS services, features, and resources that might assist FRFIs to meet certain OSFI expectations for non-financial risk management. The tables also include a link to applicable best practices in the AWS Well-Architected Framework. 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 six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability—the Well-Architected 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:

- **Requirements summary** – This column summarizes the requirements in each of the Guidelines.
- **Considerations for AWS customers** – This column explains considerations for addressing the requirements defined in the Guideline. It focuses on the customer side of the Shared Responsibility Model and outlines various AWS services, features, and resources that FRFIs can use to help them address these requirements *in* the cloud. In some cases, the table also refers to controls implemented and managed by AWS for security and compliance *of* the cloud.
- **AWS Well-Architected best practices** – This column lists best practices for security in the cloud from the AWS Well-Architected Framework that FRFIs can implement as a starting point to support their compliance efforts. Details on each best practice and associated AWS services that customers might use can be found in the AWS Well-Architected Framework.

This is not legal or compliance advice. These tables contain a non-exhaustive sample of considerations and are provided for informational purposes only. Customers are responsible for making their own independent assessments of this information, conducting appropriate due diligence, and should consult with their own legal and compliance advisors.

OSFI Guideline B-13 – Technology and Cyber Risk Management

A full analysis of Guideline B-13 is beyond the scope of this document and customers are responsible for making their own independent assessments of its requirements. This Appendix addresses some topics from sections 2 and 3 of the Guideline that FRFIs might consider relevant when using AWS.

Note: Section 1 of Guideline B-13 sets broad expectations related to technology and cyber governance, strategy, and risk management. As these are customer-specific considerations that are not directly related to a FRFI's use of AWS services, section 1 has been omitted from this guide.

Section 2: Technology Operations and Resilience

Section 2 of Guideline B-13 outlines OSFI's expectations for management and oversight of risks related to the design, implementation, management, and recovery of technology assets and services.

Section 2.1 – Technology Architecture

Principle 4: FRFIs should implement a technology architecture framework, with supporting processes to ensure solutions are built in line with business, technology, and security requirements.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.1.1: FRFIs should establish a framework of principles necessary to govern, manage, evolve, and consistently implement IT architecture across the institution in support of the enterprise's strategic technology, security and business goals and requirements.	**Customer responsibility** AWS customers can use AWS tools, services, whitepapers, technical guidance and reference materials to help them develop and maintain an architecture framework to meet OSFI's recommendations. AWS customers can access the AWS C-suite Guide to Shared Responsibility for Cloud Security and Data Safe Cloud eBook on the AWS Data Safe Cloud Checklist site to educate themselves on the benefits and risks of operating in the AWS Cloud and to help build the necessary understanding of their cyber risk environment.	OPS 4 Design for workload insights OPS 7 Operational readiness OPS 8 Workload health OPS 10 Event response

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.1.2: The scope of architecture principles should be comprehensive (for example, considers infrastructure, applications, emerging technologies, and relevant data). Using a risk-based approach, systems and associated infrastructure should be designed and implemented to achieve availability, scalability, security (Secure-by-Design), and resilience (Resilience-by-Design), commensurate with business needs.	**Customer responsibility** AWS customers can use the AWS Well-Architected Framework, which provides a consistent set of best practices for customers to evaluate architectures and questions to evaluate how well their architecture is aligned with AWS best practices. The Financial Services Industry Lens of the AWS Well-Architected Framework focuses on designing, deploying, and architecting financial services industry workloads that promote resiliency, security, and operational performance in line with risk and control objectives that FRFIs can define.	FSIOPS1 – General Design principles

Section 2.2 – Technology Asset Management

Principle 5: FRFIs should maintain an updated inventory of all technology assets supporting business processes or functions. FRFI's asset management processes should address classification of assets to facilitate risk identification and assessment, record configurations to ensure asset integrity, provide for the safe disposal of assets at the end of their life cycle, and monitor and manage technology currency.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.2.2: FRFIs should maintain a current and comprehensive asset management system, or inventory, that catalogues technology assets throughout their life cycle. Based on the FRFI's risk tolerance, this may include assets owned or leased by a FRFI, and third-party assets that store or process FRFI information or provide critical business services. The asset	**Customer responsibility** AWS customers can use the following AWS services and resources to assist them: AWS Config provides a detailed inventory of customers' AWS resources and configuration and continuously records configuration changes. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time. Amazon CloudWatch provides data and actionable insights to monitor applications, understand and respond to system-wide performance	OPS04-BP02 Implement and configure workload telemetry OPS04-BP03 Implement user activity telemetry OPS05-BP03 Use configuration management systems OPS08-BP03 Collect and analyze workload metrics

Requirements summary	Considerations for AWS customers	Well-Architected best practices
management system, or inventory, should be supported by: • Processes to categorize technology assets based on their criticality and/or classification. These processes should identify critical technology assets that are of high importance to the FRFI, or which could attract threat actors and cyber attacks, and therefore require enhanced cyber protections; and • Documented interdependencies between critical technology assets, where appropriate, to enable proper change and configuration management processes, and to assist in response to security and operational incidents, including cyber attacks.	changes, optimize resource utilization, and get a unified view of operational health. AWS Systems Manager gives visibility and control of customer infrastructure on AWS. In addition, Systems Manager provides a unified user interface to view operational data from multiple AWS services and allows automation of operational tasks across AWS resources. AWS Service Catalog allows creating and managing catalogues of IT services and infrastructure resources approved for use on AWS. In addition, customers can define and manage relationships between these resources, enabling proper change and configuration management processes. AWS resource tagging allows customers to manage, identify, organize, search, and filter resources by assigning metadata to their AWS resources. For example, security tags can contain information on confidentiality, identifying specific data confidential levels a resource supports, or compliance, like an identifier for workloads that must adhere to specific compliance requirements. AWS Resource Groups – Customers can use *resource groups* to organize their AWS resources. AWS Resource Groups lets customers simultaneously manage and automate tasks on large numbers of resources. In addition, AWS allows customers to assign metadata to many of their AWS resources as tags.	OPS08-BP04 Establish workload metrics baselines OPS08-BP06 Alert when workload outcomes are at risk OPS09-BP03 Collect and analyze operations metrics OPS09-BP07 Alert when operations anomalies are detected OPS10-BP06 Communicate status through dashboards OPS10-BP07 Automate responses to events OPS11-BP07 Perform operations metrics reviews SEC 1 Secure Operations SEC 2 Authentication SEC 3 Authorization and access control SEC 4 Security events SEC06-BP01 Perform vulnerability management SEC06-BP04 Automate compute protection

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.2.3: The technology inventory should also include a system for recording and managing asset configurations to enhance visibility and mitigate the risk of technology outages and unauthorized activity. Processes should be in place to identify, assess, and remediate discrepancies from the approved baseline configuration, and to report on breaches.	**Customer responsibility** AWS customers can use the following AWS services and resources to assist in creating an inventory system that records and manages configurations. AWS Config provides a detailed inventory of customers' AWS resources and configuration and continuously records configuration changes. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time. Using AWS Config, customers can discover resources in their account, record the configurations, and capture any changes, allowing them to troubleshoot operational issues quickly. Customers can codify compliance requirements as AWS Config rules and author remediation actions, automating the assessment of their resource configurations across their organization. Customers can evaluate resource configurations for potential vulnerabilities and review their configuration history after potential incidents to examine their security posture. AWS CloudTrail enables customers to discover and troubleshoot security and operational issues by capturing a comprehensive history of activities and changes that occurred in an AWS account within a specified period. Amazon GuardDuty continuously monitors for malicious activity and unauthorized behavior to protect customer AWS accounts and workloads. Amazon Detective automatically collects log data from AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables faster and more efficient security investigations.	OPS04-BP02 Implement and configure workload telemetry OPS07-BP01 Ensure personnel capability OPS11-BP04 Perform knowledge management OPS11-BP05 Define drivers for improvement REL06-BP02 Define and calculate metrics (Aggregation) REL06-BP06 Conduct reviews regularly SEC 1 Secure Operations SEC 2 Authentication SEC 3 Authorization and access control SEC 4 Security events SEC10-BP04 Automate containment capability SEC10-BP05 Pre-provision access SEC10-BP06 Pre-deploy tools

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.2.4: FRFIs should define standards and implement processes to ensure the secure disposal or destruction of technology assets.	**Shared responsibility** AWS tracks, documents, and verifies media sanitization and disposal actions. Media removal and disposal are performed by designated AWS personnel. Data Destruction – Content on drives is treated at the highest classification level (Critical) per AWS Data Classification policy. Classification is destroyed on storage devices as part of the decommissioning process under AWS security standards. AWS hosts are securely wiped or overwritten before provisioning for reuse. Additionally, AWS media is securely wiped or degaussed and physically destroyed before leaving AWS Secure Zones. Third-party auditors review the guidance to validate the secure wipe processes and procedures used by AWS. To help with this activity, AWS customers can use the following: AWS CloudTrail records activity in your AWS account as a CloudTrail event. Create an event data store or a trail for an ongoing record of activity and events in your AWS account. Amazon Data Lifecycle Manager automates the creation, retention, and deletion of Amazon Elastic Block Store (Amazon EBS) snapshots according to a defined policy. By configuring data lifecycle management policies, you can make sure that outdated EBS snapshots are securely deleted in compliance with your organization's standards. AWS Backup is a fully managed service that helps customers centralize and automate data protection across AWS services in the cloud and on-premises.	SEC07-BP04 Define data lifecycle management REL13-BP02 Use defined recovery strategies to meet the recovery objectives COST04-BP03 Decommission resources

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.2.5: FRFIs should continuously monitor the currency of software and hardware assets used in the technology environment in support of business processes. They should proactively implement plans to mitigate and manage risks stemming from unpatched, outdated, or unsupported assets and replace or upgrade assets before maintenance ceases.	**Shared responsibility** AWS Security performs regular vulnerability scans in the AWS environment using a variety of tools. External vulnerability assessments are conducted by an AWS approved third-party vendor at least quarterly and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers can also report issues to AWS through the AWS Vulnerability Reporting website. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring, and intrusion detection for their Amazon EC2 and Amazon Elastic Container Service (Amazon ECS) instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans. Amazon Inspector is a vulnerability management service that continuously scans AWS workloads for software vulnerabilities and unintended network exposure. As Amazon Inspector collects information about a customer's environment through scans, it provides severity scores tailored to the environment. Amazon Inspector examines the security metrics that compose the National Vulnerability Database (NVD) base score for a vulnerability and adjusts them according to the customer's computing environment. For example, the service might lower the Amazon Inspector score of a finding for an Amazon EC2 instance if the vulnerability is exploitable over the network. Still, no open network path to the internet is available from the instance.	OPS05-BP05 Perform patch management OPS08-BP06 Alert when workload outcomes are at risk OPS08-BP07 Alert when workload anomalies are detected OPS09-BP03 Collect and analyze operations metrics OPS09-BP07 Alert when operations anomalies are detected REL08-BP01 Use runbooks for standard activities such as deployment REL08-BP04 Deploy using immutable infrastructure REL08-BP05 Deploy changes with automation SEC05-BP01 Create network layers SEC05-BP02 Control traffic at all layers SEC05-BP03 Automate network protection SEC05-BP04 Implement inspection and protection

Requirements summary	Considerations for AWS customers	Well-Architected best practices
	The Amazon Inspector dashboard offers a high-level view of findings from across a customer's environment. From the dashboard, the customer can access the granular details of a finding. The dashboard contains streamlined information about scan coverage in the environment, the most critical findings, and which resources have the most findings. The risk-based remediation panel in the Amazon Inspector dashboard presents the findings that affect the most significant number of instances and images. This panel makes it easier to identify the findings with the most significant impact on the environment, review finding details, and review suggested solutions. Customers should perform regular patching operations for resolving vulnerabilities identified by Amazon Inspector based on the severity of the vulnerabilities. Customers can use AWS Systems Manager Patch Manager to automate the process of patching nodes. There might be zero-day or other high and critical severity vulnerabilities where patches are available. However, customers might not want to wait for the regular patching schedule to remediate them. In these cases, on-demand mechanisms for patching should exist. Customers can use AWS Systems Manager Automation Runbook for on-demand Amazon Inspector vulnerability findings remediation.	SEC06-BP01 Perform vulnerability management SEC06-BP02 Reduce attack surface SEC06-BP03 Implement managed services SEC06-BP04 Automate compute protection SEC10-BP02 Develop incident management plans SEC11-BP02 Automate testing throughout the development and release lifecycle SUS06-BP02 Keep your workload up-to-date

Purposely left blank.

Section 2.4 – System Development Life Cycle

Principle 7: FRFIs should implement a system development life cycle (SDLC) framework for the secure development, acquisition and maintenance of technology systems that perform as expected in support of business objectives.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.4.2: In addition to the general technology processes and controls, FRFIs should establish control gates to ensure that security requirements and expectations are embedded in each phase of the SDLC. For Agile software development methods, FRFIs should continue to incorporate the necessary SDLC and security-by-design principles throughout their Agile process.	**Customer responsibility** Continuous integration and continuous delivery (CI/CD) are essential to enable rapid software changes while maintaining system stability and security. AWS offers various tools to help FRFIs build their CI/CD capabilities as a set of developer services. AWS CodeStar – This service provides a centralized interface for managing software development projects using various methodologies such as Agile and Waterfall. Customers can use AWS CodeStar to create project templates that include source control, build, test, and deployment configurations, helping them maintain a consistent and controlled SDLC process. AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy, and AWS CodePipeline – These services enable customers to create and manage the various stages of the SDLC, including source control, build, test, and deployment. By integrating these services, customers can automate their development pipeline and know that their software is developed, tested, and deployed in a controlled and secure manner. AWS Well-Architected Framework –This framework provides best practices and design principles for building secure, high-performing, resilient infrastructure. By following the guidelines in the Well-Architected Framework, customers can know that their software development processes align with industry standards and support their business objectives. AWS CloudFormation – This service allows customers to model and provision AWS resources using code, enabling them to define the infrastructure needed to support their applications throughout the SDLC.	OPS05-BP01 Use version control OPS05-BP02 Test and validate changes OPS05-BP03 Use configuration management systems OPS05-BP04 Use build and deployment management systems OPS06-BP03 Use deployment management systems OPS11-BP08 Document and share lessons learned REL08-BP01 Use runbooks for standard activities such as deployment PERF01-BP07 Load test your workload REL10-BP01 Deploy the workload to multiple locations REL12-BP05 Test resiliency using chaos engineering REL13-BP04 Manage configuration drift at the DR site or Region

Requirements summary	Considerations for AWS customers	Well-Architected best practices
	By using CloudFormation templates, they can maintain consistency and control over their infrastructure resources. Amazon CloudWatch and AWS X-Ray: These monitoring services enable you to track application performance and identify issues throughout the SDLC. By monitoring key performance metrics and using distributed tracing, you can know that your systems and software perform as expected to support your business objectives. AWS Security Services – Services such as Amazon GuardDuty, AWS WAF, and AWS Shield help ensure the security of your applications throughout the SDLC. Integrating these services into your development pipeline allows you to identify and remediate potential security vulnerabilities before they impact your production environment. AWS CodeArtifact – This fully managed artifact repository service allows customers to securely store and share software packages used in their development process. By using CodeArtifact, customers can maintain control over their software dependencies and know that dependencies are managed securely and competently.	SEC01-BP06 Automate testing and validation of security controls in pipelines SEC06-BP04 Automate compute protection SEC08-BP05 Use mechanisms to keep people away from data SEC11-BP02 Automate testing throughout the development and release lifecycle SEC11-BP04 Manual code reviews SUS06-BP01 Adopt methods that can rapidly introduce sustainability improvements
Section 2.4.3: By integrating application security controls and requirements into software development and technology operations, new software and services can be delivered rapidly without compromising application security. When these practices are employed, FRFIs should ensure they are aligned with the SDLC framework and applicable technology and cyber policies and standards.	**Customer responsibility** To limit a development team's access to only the resources they need, customers can use AWS Identity and Access Manager (IAM) and AWS Organizations to centrally govern and manage multiple accounts as they scale their AWS workloads. With AWS Organizations, administrators can use service control policies (SCPs) to establish permission guardrails that all users and roles in the organization's accounts adhere to.	OPS01-BP03 Evaluate governance requirements OPS02-BP01 Resources have identified owners SEC01-BP01 Separate workloads using accounts SEC01-BP06 Automate testing and validation of security controls in pipelines

Requirements summary	Considerations for AWS customers	Well-Architected best practices
		SEC03-BP05 Define permission guardrails for your organization SEC03-BP07 Analyze public and cross-account access SEC03-BP08 Share resources securely within your organization SEC07-BP02 Define data protection controls COST02-BP03 Implement an account structure
Section 2.4.4: For software and systems that are acquired, FRFIs should ensure that security risk assessments are conducted, and that systems implementation is subject to the control requirements as required by the FRFI's SDLC framework.	**Shared responsibility** 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. AWS monitors and escalates risks on a continuous basis, regularly performing risk assessments on newly implemented controls. While the security risk assessment of acquired systems and software is an action for the FRFI to complete independently, a number of AWS resources and services described throughout this document are available to help customers to perform the assessment if the acquired system or software is running on AWS.	SEC06-BP01 Perform vulnerability management SEC06-BP04 Automate compute protection SEC06-BP05 Enable people to perform actions at a distance SEC08-BP05 Use mechanisms to keep people away from data OPS05-BP03 Use configuration management systems OPS05-BP05 Perform patch management

Requirements summary	Considerations for AWS customers	Well-Architected best practices
		OPS07-BP03 Use runbooks to perform procedures OPS07-BP04 Use playbooks to investigate issues REL06-BP04 Automate responses (Real-time processing and alarming) COST02-BP06 Track project lifecycle

Purposely left blank.

Section 2.5 – Change and Release Management

Principle 8: FRFIs should establish and implement a technology change and release management process and supporting documentation to ensure changes to technology assets are conducted in a controlled manner that ensures minimal disruption to the production environment.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.5.1: FRFIs should ensure that changes to technology assets in the production environment are documented, assessed, tested, approved, implemented, and verified in a controlled manner. The change and release management standard should outline the key controls required throughout the change management process. The standard should also define emergency change and control requirements to ensure that such changes are implemented in a controlled manner with adequate safeguards.	**Customer responsibility** AWS customers can use the following AWS services and resources to assist in creating an inventory system that records and manages configurations: AWS Config provides a detailed inventory of customers' AWS resources and configuration and continuously records configuration changes. This includes how the resources are related to one another and how they were configured in the past so that customers can see how the configurations and relationships change over time. AWS Systems Manager Change Manager is an enterprise change management framework for requesting, approving, implementing, and reporting operational changes to application configuration and infrastructure. CI/CD is crucial for verifying that changes to technology assets in the production environment are carefully managed. By promoting changes through CI/CD, the system captures a clear record of modifications, aiding troubleshooting and knowledge sharing. It enables assessment and validation through automated tests and quality checks, catching potential issues early on.	OPS02-BP06 Mechanisms exist to request additions, changes, and exceptions OPS05-BP04 Use build and deployment management systems OPS06-BP02 Test and validate changes OPS06-BP03 Use deployment management systems
Section 2.5.2: Segregation of duties is a key control used in protecting assets from unauthorized changes. FRFIs should segregate duties in the change management process to ensure that the same person cannot develop,	**Customer responsibility** AWS Organizations is an account management service that enables customers to consolidate multiple AWS accounts into an *organization* that they create and centrally manage. Within an organization, customers can create organization units (OUs) to group AWS accounts that they want to apply security policies to and manage as	SEC02-BP02 Use temporary credentials SEC02-BP04 Rely on a centralized identity provider SEC03-BP05 Define permission guardrails for your organization

Requirements summary	Considerations for AWS customers	Well-Architected best practices
authorize, execute, and move code or releases between production and non-production technology environments.	a whole. For example, customers typically create separate OUs to group production and non-production AWS accounts. AWS Organizations is integrated with AWS IAM Identity Center, through which customers can manage sign-in security for their *workforce identities*, also known as workforce users. IAM Identity Center provides one place where customers can create or connect workforce users and centrally manage their access across all their AWS accounts and applications. Customers can use *multi-account permissions* to assign their workforce users access to AWS accounts. This allows customers to segregate duties so that the same person doesn't have access to both non-production and production AWS accounts.	
Section 2.5.3: Controls should be implemented to ensure traceability and integrity of the change record as well as the asset being changed (for example, code, releases) in each phase of the change management process.	**Customer Responsibility** AWS CodeCommit is a secure, highly scalable, managed source control service that hosts private Git repositories. CodeCommit eliminates the need for customers to manage their own source control system or worry about scaling its infrastructure. AWS CodeArtifact is a secure, highly scalable, managed artifact repository service that helps organizations store and share software packages for application development. Customers can use CodeArtifact with popular build tools and package managers such as the NuGet CLI, Maven, Gradle, npm, yarn, pip, and twine. CodeArtifact helps reduce the need for customers to manage their own artifact storage system or worry about scaling its infrastructure. AWS CloudTrail is an AWS service that helps customers enable operational and risk auditing, governance, and compliance of their AWS account. Actions taken by a user, role, or AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface (AWS CLI), and	OPS04-BP04 Implement dependency telemetry OPS04-BP05 Implement transaction traceability REL06-BP07 Monitor end-to-end tracing of requests through your system SUS04-BP05 Remove unneeded or redundant data

Requirements summary	Considerations for AWS customers	Well-Architected best practices
	AWS SDKs and APIs. With CloudTrail, customers can configure central logging of actions performed across their organization.	

Section 2.6 – Patch Management

Principle 9: FRFIs should implement patch management processes to ensure controlled and timely application of patches across their technology environments to address vulnerabilities and flaws.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.6.1: The patch management process should define clear roles and responsibilities for all stakeholders involved. Patching should follow the FRFI's existing change management processes, including emergency change processes. Patches should be tested before deployment to the production environment.	**Shared responsibility** AWS Security performs regular vulnerability scans in the AWS environment using a variety of tools. External vulnerability assessments are conducted by an AWS approved third-party vendor at least quarterly, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers can also report issues to AWS through the AWS Vulnerability Reporting website. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring, and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Systems Manager Patch Manager automates patching managed nodes with security-related and other updates. Customers can use Patch Manager to apply patches for both operating systems and applications.	OPS03-BP04 Communications are timely, clear, and actionable OPS05-BP05 Perform patch management OPS05-BP06 Share design standards REL08-BP05 Deploy changes with automation SEC06-BP01 Perform vulnerability management SUS06-BP02 Keep your workload up-to-date

Requirements summary	Considerations for AWS customers	Well-Architected best practices
	Patch Manager uses patch baselines, including rules for auto-approving patches within days of release and a list of approved and rejected patches. Customers can install patches regularly by scheduling patching to run as a Systems Manager maintenance window task. Patches can be installed individually or in large groups of managed nodes using tags (tags are keys that help identify and sort resources within an organization). Customers can add tags to their patch baselines when creating or updating them. Patch Manager provides options to scan managed nodes and report compliance on a schedule, install available patches on a schedule, and patch or scan targets on demand whenever needed. Customers can also generate patch compliance reports sent to an S3 bucket of their choice. In addition, customers can generate one-time reports or create reports on a regular schedule. Patch Manager integrates with IAM, CloudTrail, and Amazon EventBridge to provide a secure patching experience that includes event notifications and the ability to audit usage.	

Purposely left blank.

Section 2.7 – Incident and Problem Management

Principle 10: FRFIs should effectively detect, log, manage, resolve, monitor, and report on technology incidents and minimize their impacts.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.7.1: FRFIs should define standards and implement processes for incident and problem management. Standards should provide an appropriate governance structure for timely identification and escalation of incidents, restoration and/or recovery of an affected system, and investigation and resolution of incident root causes.	**Shared responsibility** Developing and implementing mechanisms and plans to detect and respond to information security incidents is a shared responsibility between AWS and FRFIs. The effectiveness of AWS controls for its portion of these shared responsibilities is described in the assurance reports available in AWS Artifact. The AWS Security Incident Response Guide presents an overview of the fundamentals of responding to security incidents within a customer's AWS Cloud environment. It focuses on an overview of cloud security and incident response concepts and identifies cloud capabilities, services, and mechanisms available to customers responding to security issues. AWS Enterprise Support provides customers with concierge-like service where the focus is helping them achieve their outcomes and find success in the cloud. With Enterprise Support, customers get 24/7 technical support from high-quality engineers, tools, and technology to automatically manage the health of their environment. Customers also get access to a Technical Account Manager (TAM) who provides consultative architectural and operational guidance delivered in the context of their applications and use cases to help them achieve the greatest value from AWS.	OPS01-BP05 Evaluate threat landscape OPS07-BP03 Use runbooks to perform procedures OPS07-BP06 Create support plans for production workloads OPS10-BP01 Use a process for event, incident, and problem management SEC10-BP01 Identify key personnel and external resources SEC10-BP02 Develop incident management plans SEC10-BP03 Prepare forensic capabilities SEC10-BP05 Pre-provision access SEC10-BP06 Pre-deploy tools SEC10-BP07 Run game days

Requirements summary	Considerations for AWS customers	Well-Architected best practices
		COST01-BP01 Establish a cost optimization function COST01-BP04 Implement cost awareness in your organizational processes
Section 2.7.2: FRFIs should implement processes and procedures for managing technology incidents; elements may include: • Defining and documenting roles and responsibilities of relevant internal and external parties to support effective incident response; • Establishing early warning indicators or triggers of system disruption (that is, detection) that are informed by ongoing threat assessment and risk surveillance activities; • Identifying and classifying incidents according to priority, based on their impacts on business services;	**Customer responsibility** While definition of information security-related roles and responsibilities is an action for FRFIs to complete independently, a number of AWS resources and services are available to help customers meet these requirements. A common theme among the most successful AWS customers is that they have an engaged board and senior management team who are both enthusiastic about the benefits of moving to the cloud and aware of the changed risks and responsibilities of operating in the cloud. The AWS C-suite Guide to Shared Responsibility for Cloud Security and the Data Safe Cloud eBook can inform boards and senior management about the cloud's benefits and risks.	REL10-BP01 Deploy the workload to multiple locations REL10-BP02 Select the appropriate locations for your multi-location deployment REL11-BP02 Fail over to healthy resources REL12-BP02 Perform post-incident analysis REL13-BP02 Use defined recovery strategies to meet the recovery objectives SEC01-BP01 Separate workloads using accounts SEC01-BP02 Secure account root user and properties SEC02-BP01 Use strong sign-in mechanisms

Requirements summary	Considerations for AWS customers	Well-Architected best practices
• Developing and implementing incident response procedures that mitigate the impacts of incidents, including internal and external communication actions that contain escalation and notification triggers and processes; • Performing periodic testing and exercises using plausible scenarios in order to identify and remedy gaps in incident response actions and capabilities; • Conducting periodic exercises and testing of incident management process, playbooks, and other response tools (for example, coordination and communication) to validate and maintain their effectiveness; and; • Establishing and periodically testing incident management processes with third parties.		SEC02-BP04 Rely on a centralized identity provider SEC02-BP05 Audit and rotate credentials periodically SEC03-BP01 Define access requirements SEC03-BP03 Establish emergency access process SEC03-BP04 Reduce permissions continuously SEC03-BP07 Analyze public and cross-account access SEC10-BP05 Pre-provision access
Section 2.7.3: FRFIs should develop problem management processes that provide for the detection, categorization, investigation, and resolution of suspected incident	**Customer responsibility** The following is a list of AWS services that FRFIs can use to support detection and response of incidents.	OPS07-BP04 Use playbooks to investigate issues

Requirements summary	Considerations for AWS customers	Well-Architected best practices
causes. Processes should include post-incident reviews, root cause and impact diagnostics, and identification of trends or patterns in incidents. Problem management activities and findings should inform related control processes and be used on an ongoing basis to improve incident management processes and procedures, including change and release management.	AWS CloudTrail, customers can discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in an AWS account within a specified period. AWS Config allows customers to continuously audit and assess the overall compliance of AWS resource configurations with organizational policies and guidelines. Amazon GuardDuty is a threat detection service that continuously monitors malicious activity and unauthorized behavior to protect customer AWS accounts and workloads. Amazon Detective automatically collects log data from AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables faster and more efficient security investigations. AWS Security Hub provides a comprehensive view of customers' high-priority security alerts and compliance status across AWS accounts. With Security Hub, customers have a single place that aggregates, organizes, and prioritizes security alerts or findings from multiple AWS services.	OPS10-BP01 Use a process for event, incident, and problem management REL06-BP06 Conduct reviews regularly REL12-BP01 Use playbooks to investigate failures SEC04-BP01 Configure service and application logging SEC04-BP03 Automate response to events SEC04-BP04 Implement actionable security events SEC10-BP03 Prepare forensic capabilities SEC10-BP05 Pre-provision access

Purposely left blank.

Section 2.8 – Technology Service Measurement and Monitoring

Principle 11: FRFIs should develop service and capacity standards and processes to monitor operational management of technology, ensuring business needs are met.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.8.1: FRFIs should establish technology service management standards with defined performance indicators and/or service targets that can be used to measure and monitor the delivery of technology services. Processes should also provide for remediation where targets are not being met.	**Customer responsibility** Operations Management is a suite of capabilities that helps you keep track of your AWS resources across AWS Regions and accounts. These capabilities can assist you in effectively managing your AWS resources to ensure your technology infrastructure meets business needs. Operations Management offers several main capabilities: AWS Systems Manager OpsCenter is the central location for operations engineers and system administrators to view, track, investigate, and resolve operational work items (OpsItems) related to AWS resources. This Systems Manager capability aggregates and standardizes OpsItems across services while providing contextual investigation data about each OpsItem, related OpsItems, and related resources. OpsCenter also provides Systems Manager automation documents (runbooks) that customers can use to resolve issues quickly. Amazon CloudWatch dashboards are customizable home pages in the CloudWatch console. They let customers access and view data from the Systems Manager to monitor their resources, including centrally monitoring resources in different Regions. Customers can use CloudWatch dashboards to create customized views of the metrics and alarms for their AWS resources. AWS Trusted Advisor and AWS Personal Health dashboards are tools to help customers monitor different aspects of the health of their resources. Trusted Advisor is an online tool that provides real-time guidance to help customers provision their resources following AWS best practices. The AWS Health Dashboard provides information about AWS Health events that can affect customers' accounts. Systems Manager Incident Manager assists in managing incidents occurring in customers' AWS-hosted applications. Incident Manager combines user	OPS01-BP05 Evaluate threat landscape OPS10-BP01 Use a process for event, incident, and problem management OPS10-BP06 Communicate status through dashboards OPS11-BP03 Implement feedback loops REL01-BP01 Aware of service quotas and constraints REL01-BP02 Manage service quotas across accounts and regions REL01-BP03 Accommodate fixed service quotas and constraints through architecture REL03-BP02 Build services focused on specific business domains and functionality

Requirements summary	Considerations for AWS customers	Well-Architected best practices
	engagements, escalation, runbacks, response plans, chat channels, and post-incident analysis to help customers triage incidents faster and return their applications to normal.	REL11-BP07 Architect your product to meet availability targets and uptime service level agreements (SLAs) REL12-BP02 Perform post-incident analysis COST02-BP02 Implement goals and targets
Section 2.8.2: FRFIs should define performance and capacity requirements with thresholds on infrastructure utilization. These requirements should be continuously monitored against defined thresholds to ensure technology performance and capacity support current and future business needs.	**Customer responsibility** It's essential that customers measure performance and ensure they don't reach capacity limits. Although the AWS Cloud can allow customers to scale to unparalleled levels, it's essential to understand that performance considerations and service quotas need to be measured and acted upon. Amazon CloudWatch monitors the AWS resources and the applications customers run on AWS in real-time. Customers can use CloudWatch to collect and track metrics, which are variables they can measure for their resources and applications. Customers can create alarms that watch metrics and send notifications or automatically change the resources they monitor when a threshold is breached. For example, they can monitor the CPU usage and disk reads and writes of their EC2 instances and then use that data to determine whether they should launch additional instances to handle the increased load. Though the cloud offers virtually infinite scalability, it's essential to remember that managed services have quotas (formerly referred to as limits) designed to help guarantee the availability of AWS resources and prevent accidental provisioning of more resources than needed. To anticipate demand in production, customers must anticipate these quotas by running load tests in pre-production environments.	OPS07-BP06 Create support plans for production workloads REL01-BP03 Accommodate fixed service quotas and constraints through architecture REL01-BP04 Monitor and manage quotas REL01-BP05 Automate quota management REL01-BP06 Ensure that a sufficient gap exists between the current quotas and the maximum usage to accommodate failover

Requirements summary	Considerations for AWS customers	Well-Architected best practices
	AWS Service Quotas is a service that enables customers to view and manage their quotas for AWS services from a central location. Along with looking up the quota values, they can also request a quota increase, monitor the usage of specific services API actions, and create alerts for them directly from the Service Quotas console. In addition, AWS Trusted Advisor gives customers additional insight into whether they are approaching or breaching limits.	SEC03-BP07 Analyze public and cross-account access COST01-BP05 Report and notify on cost optimization COST04-BP01 Track resources over their lifetime COST06-BP03 Select resource type, size, and number automatically based on metrics COST06-BP01 Perform cost modeling SUS03-BP02 Remove or refactor workload components with low or no use

Purposely left blank.

Section 2.9 – Disaster Recovery

Principle 12: FRFIs should establish and maintain an enterprise disaster recovery program (EDRP) to support their ability to deliver technology services through disruption and operate within their risk tolerance.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 2.9.1: FRFIs should develop, implement, and maintain an ERDP that sets out their approach to recovering technology services during a disruption. FRFIs should align the disaster recovery program with their business continuity management program. The EDRP should establish: • Accountability and responsibility for the availability and recovery of technology services, including recovery actions; • A process for identifying and analyzing technology services and key dependencies required to operate within the FRFI's risk tolerance; • Plans, procedures, and/or capabilities to recover technology services to an acceptable level, within an acceptable timeframe, as defined and prioritized by the FRFI; and,	**Customer responsibility** Disaster recovery (DR) is an essential aspect of resiliency strategies in the cloud as it deals with how workloads respond when a disaster occurs, defined as an event that causes a significant negative impact on the business. To address DR, organizations must consider their business objectives and implement resilience in the design of their workloads to meet their recovery objectives, known as the recovery point objective (RPO) and recovery time objective (RTO), respectively, for a given one-time disaster event. This approach helps maintain business continuity as part of business continuity planning (BCP). AWS Disaster Recovery is a collection of AWS services and solutions that help customers to recover their IT systems and data quickly and efficiently in case of a disaster. It enables customers to implement DR solutions for their on-premises infrastructure or their workloads running on AWS. AWS offers a range of DR services that can help organizations replicate their data and applications to a secondary location, enabling them to recover quickly in the event of a disaster. These services include AWS Storage Gateway, Amazon S3, Amazon EBS, and AWS Elastic File System (EFS). AWS also provides AWS Elastic Disaster Recovery, a fully managed service that simplifies setting up and managing DR solutions. Elastic Disaster Recovery automates the replication of data and applications and provides continuous monitoring and testing of the disaster recovery environment. This helps customers to meet their RTO and RPO requirements and maintain that their business-critical applications are always available. Before implementing a DR plan, organizations must perform a business impact analysis and risk assessment to determine the business impact of a disruption to their workloads. The analysis should identify the impact on internal and external customers of being unable to use the workloads and its effect on the business.	REL09-BP01 Identify and back up all data that needs to be backed up, or reproduce the data from sources REL09-BP03 Perform data backup automatically REL09-BP04 Perform periodic recovery of the data to verify backup integrity and processes REL10-BP02 Select the appropriate locations for your multi-location deployment REL10-BP03 Automate recovery for components constrained to a single location REL13-BP02 Use defined recovery strategies to meet the recovery objectives

Requirements summary	Considerations for AWS customers	Well-Architected best practices
• A policy or standard with controls for data back-up and recovery processes, requirements for data storage, and periodic testing.	Additionally, the analysis should determine how quickly the workload needs to be made available and how much data loss can be tolerated. Recovery objectives should be made in conjunction with the probability of disruption and cost of recovery to inform the business value of disaster recovery for a workload. Organizations might consider deploying infrastructure across multiple regions for highly critical workloads with data replication and continuous backups to minimize business impact. Disaster recovery strategies evolve with technical innovation, and DR plans on-premises might involve physically transporting tapes or replicating data to another site. However, DR in the AWS Cloud offers several advantages over traditional environments, such as reduced complexity, simple and repeatable testing, lower management overhead, automation opportunities, and reduced cost.	REL13-BP03 Test disaster recovery implementation to validate the implementation REL13-BP05 Automate recovery
Section 2.9.2: FRFIs should manage key dependencies required to support the EDRP, such as: • Information security requirements for data security and storage (for example, encryption); and, • Location of technology asset centers, backup sites, service provider locations and proximity to primary data centers, and other critical technology assets and locations.	**Customer responsibility** AWS provides various services that maintain secure backup and restoration practices. For instance, IAM is a service that provides authentication and authorization to control and detect access to backups. Encryption is also used to help prevent and detect compromised data integrity of backups. Amazon S3, one of the cloud storage services provided by AWS, supports multiple encryption methods to secure data at rest. Server-side encryption and client-side encryption are the two methods customers can use. Customers can also use AWS Key Management Service (AWS KMS) to create and store data keys and IAM to set policies on who can access their data keys and decrypted data. If customers encrypted their databases on Amazon RDS, their backups are also encrypted. DynamoDB backups are always encrypted. Securing backups and encrypting data is crucial to prevent tampering and unauthorized access. Establish this best practice to avoid exposing a high level of risk. To implement secure backup and restoration practices, it's advisable that customers encrypt each of their data stores, enable encryption in RDS, EBS volumes, DynamoDB, and Amazon EFS, and configure encryption in the source and	PERF03-BP01 Understand storage characteristics and requirements PERF03-BP02 Evaluate available configuration options PERF04-BP01 Understand data characteristics PERF03-BP03 Make decisions based on access patterns and metrics REL09-BP02 Secure and encrypt backups

Requirements summary	Considerations for AWS customers	Well-Architected best practices
	destination Regions. Following security best practices, customers should also limit access to backups, snapshots, and replicas with the least privileged permissions. AWS offers a range of disaster recovery strategies broadly classified into four categories. The simplest and most cost-effective approach involves making backups. More complex options involve using multiple active Regions. Active/passive strategies use an active site to host the workload and a passive site for recovery. It's essential that customers assess and test their disaster recovery plan regularly—AWS Resilience Hub can help with this by continuously monitoring the resilience of customers' workloads. AWS takes care of data center connectivity, power, air conditioning, fire suppression, and hardware, giving customers access to multiple fault-isolated Availability Zones, each consisting of one or more data centers. By deploying across multiple Availability Zones within a single AWS Region, customers can mitigate against natural and technical disasters. In addition, partitioning workloads across multiple zones in the same region further increases resilience. To protect against the failure of a single or multiple data centers, customers can deploy their workload across multiple Availability Zones in a single AWS Region and back up data and configuration to another Region. This strategy simplifies disaster recovery plans and reduces costs. Availability Zones within a Region can also be used as discrete locations for workloads with regulatory data residency requirements. It's essential to understand how AWS provides physical redundancy and resilience by designing each Region with multiple Availability Zones. Customers can use this infrastructure to achieve high availability and uninterrupted performance even during power outages, internet downtime, floods, and other natural disasters.	SUS04-BP06 Use shared file systems or storage to access common data SEC02-BP03 Store and use secrets securely SEC07-BP03 Automate identification and classification SEC08-BP01 Implement secure key management SEC08-BP02 Enforce encryption at rest SEC08-BP03 Automate data at rest protection SEC09-BP02 Enforce encryption in transit SEC09-BP03 Automate detection of unintended data access
Section 2.9.3: To promote learning, continuous improvement, and technology resilience, FRFIs should regularly validate and report on their	**Customer responsibility** Disaster recovery is crucial for any business, and AWS Elastic Disaster Recovery is a reliable solution to make sure that customer applications and data are always available. With this service, customers can perform non-disruptive tests to confirm	OPS03-BP04 Communications are timely, clear, and actionable

Requirements summary	Considerations for AWS customers	Well-Architected best practices
disaster recovery strategies, plans, and/or capabilities against severe but plausible scenarios. These scenarios should be forward-looking and consider, where appropriate: • New and emerging risks or threats; • Material changes to business objectives or technologies; • Situations that can lead to prolonged outage; and, • Previous incident history and known technology complexities or weaknesses. FRFIs' disaster recovery scenarios should test: • The FRFI's backup and recovery capabilities and processes to validate resiliency strategies, plans, and actions, and confirm the organization's ability to meet pre-defined requirements; and,	that implementation is complete and maintain readiness by monitoring replication and periodically performing non-disruptive recovery and failback drills. When launching instances for drills or recovery, Elastic Disaster Recovery automatically converts customer's servers to boot and runs natively on AWS, providing a seamless transition. Customers can launch recovery instances on AWS within minutes, using the most up-to-date server state or a previous point in time. After customer applications run on AWS, they can keep the applications there, or they can initiate data replication back to their primary site when the issue is resolved. Performing frequent drills is critical to ensure you're always prepared for a disaster. Elastic Disaster Recovery makes it simple for customers to launch drill instances as frequently as they want. These drills are non-disruptive, meaning they won't impact the source server or ongoing data replication. If customers experience a disaster in the middle of a drill, they can launch a new recovery instance from the source server's current state. Additionally, customers can use playbooks to identify issues and enable consistent and prompt responses to failure scenarios. Playbooks are documented processes that contain the information and guidance necessary for an adequately skilled person to gather applicable information, identify potential sources of failure, isolate faults, and determine contributing factors. By documenting processes in playbooks, customers can ensure consistent and prompt responses to failure scenarios. Implementing playbooks as code and scripting playbooks is also recommended to verify consistency and reduce errors caused by manual processes. Playbooks can be composed of multiple scripts representing the steps necessary to identify the contributing factors to an issue. Runbook activities can be initiated or performed as part of playbook activities or might prompt the running of a playbook in response to identified events. Finally, you can automate your operational playbooks with AWS Systems Manager, AWS Lambda, Amazon EventBridge, and Amazon CloudWatch alarms, making	OPS07-BP03 Use runbooks to perform procedures OPS07-BP04 Use playbooks to investigate issues REL06-BP04 Automate responses (Real-time processing and alarming) REL09-BP01 Identify and back up all data that needs to be backed up, or reproduce the data from sources REL09-BP03 Perform data backup automatically REL09-BP04 Perform periodic recovery of the data to verify backup integrity and processes REL10-BP02 Select the appropriate locations for your multi-location deployment REL10-BP03 Automate recovery for components constrained to a single location

Requirements summary	Considerations for AWS customers	Well-Architected best practices
• Critical third-party technologies and integration points with upstream and downstream dependencies, including both on- and off-premises technology.	managing and running disaster recovery plans easier. With these tools, customers can be confident that their systems and data will be protected in a disaster.	REL12-BP01 Use playbooks to investigate failures REL13-BP02 Use defined recovery strategies to meet the recovery objectives REL13-BP03 Test disaster recovery implementation to validate the implementation REL13-BP05 Automate recovery

Section 3: Cyber Security

Section 3 of Guideline B-13 follows the structure of the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity and outlines OSFI's expectations for management and oversight of cyber risk.

Section 3.1 – Identify

Principle 14: FRFIs should maintain a range of practices, capabilities, processes, and tools to identify and assess cyber security for weaknesses that could be exploited by external and internal threat actors.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.1.1: FRFIs should identify current or emerging cyber threats proactively using threat assessments to evaluate threats and assess security risk. This includes implementing information and cyber security threat and risk assessments, processes, and tools to cover controls at different layers of defense.	**Customer responsibility** AWS customers might use Amazon GuardDuty which is a threat detection service that continuously monitors for malicious activity and anomalous behavior to protect customers' AWS accounts, workloads, Kubernetes clusters, and data stored in Amazon S3. Amazon GuardDuty looks for atypical API requests, unapproved deployments, and access credentials that might suggest a potential account reconnaissance or breach.	OPS01-BP05 Evaluate threat landscape SEC01-BP03 Identify and validate control objectives SEC01-BP04 Keep up-to-date with security threats SEC01-BP07 Identify threats and prioritize mitigations using a threat model SEC06-BP01 Perform vulnerability management SEC11-BP01 Train for application security

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.1.2: FRFIs should adopt a risk-based approach to threat assessment and testing. FRFIs should set defined triggers, and minimum frequencies, for intelligence-led threat assessments to test cyber security processes and controls. FRFIs should also regularly perform tests and exercises to identify vulnerabilities or control gaps in their cyber security programs (for example, penetration testing and red teaming) using an intelligence-led approach. The scope and potential impacts of such testing should be clearly defined by the FRFI with effective risk mitigation controls applied throughout the assessment to manage any associated inherent risks.	**Customer responsibility** The Well-Architected Framework emphasizes learning, measuring, and improving. It provides a consistent approach for evaluating architectures and implementing designs that will scale over time. AWS provides the AWS Well-Architected Tool to help customers review their approach before development, the state of their workloads before production, and the state of their workloads in production. Customers can compare their workloads to the latest AWS architectural best practices, monitor the overall status of the workloads, and gain insight into potential risks. AWS Trusted Advisor is a tool that provides access to a core set of checks that recommend optimizations that might help shape customers' priorities. Business and Enterprise Support customers receive access to additional checks focusing on security, reliability, performance, and cost optimization that can further help shape their priorities.	OPS01-BP05 Evaluate threat landscape SEC01-BP03 Identify and validate control objectives SEC01-BP04 Keep up-to-date with security threats SEC01-BP07 Identify threats and prioritize mitigations using a threat model SEC04-BP03 Automate response to events SEC04-BP04 Implement actionable security events SEC05-BP03 Automate network protection SEC05-BP04 Implement inspection and protection SEC06-BP01 Perform vulnerability management SEC11-BP01 Train for application security SEC11-BP08 Build a program that embeds security ownership in workload teams

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.1.3: FRFIs should establish processes to conduct regular vulnerability assessments of their technology assets, including but not limited to network devices, systems, and applications. Processes should articulate the frequency with which vulnerability scans and assessments are conducted. FRFIs should assess and rank relevant cyber vulnerabilities and threats according to the severity of the threat and risk exposure to technology assets using a standard risk measurement methodology. In doing so, FRFIs should consider the potential cumulative impact of vulnerabilities, irrespective of risk level, that could present a high-risk exposure when combined.	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them: Amazon Inspector is a vulnerability management service that continuously scans AWS workloads for software vulnerabilities and unintended network exposure. As Amazon Inspector collects information about an environment through scans, it provides severity scores tailored to the environment. Customers can use the Amazon Inspector risk score to prioritize remediation actions efficiently. The Amazon Inspector dashboard offers a high-level view of findings from across an environment. The risk-based remediation panel in the Amazon Inspector dashboard presents the findings that affect the most significant number of EC2 instances and container images. This panel makes it easier for customers to identify the findings with the most significant impact on their environment, review finding details, and review suggested solutions. AWS Security Hub is a cloud security posture management service that performs automated, continuous security best practice checks against AWS resources. In addition, security Hub aggregates security alerts (that is, findings) from various AWS services and partner products in a standardized format so that customers can take action more quickly. When Security Hub is activated, Amazon Inspector will also publish findings to Security Hub.	SEC04-BP02 Analyze logs, findings, and metrics centrally SEC05-BP01 Create network layers SEC05-BP03 Automate network protection SEC05-BP04 Implement inspection and protection SEC06-BP01 Perform vulnerability management SEC06-BP02 Reduce attack surface SEC07-BP03 Automate identification and classification SEC09-BP03 Automate detection of unintended data access SEC10-BP02 Develop incident management plans SEC11-BP02 Automate testing throughout the development and release lifecycle REL06-BP01 Monitor all components for the workload (Generation)

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.1.4: FRFIs should ensure that adequate controls are in place to identify, classify, and protect structured and unstructured data based on their confidentiality classification. FRFIs should implement processes to perform periodic discovery scans to identify changes and deviations from established standards and controls to protect data from unauthorized access.	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them: Amazon Macie can help customers inventory and classify sensitive and business-critical data stored in AWS. Macie uses machine learning (ML) to automate data discovery, classifying, labelling, and applying protection rules. As a result, customers can better understand where sensitive information is stored and how it's being accessed, including user authentications and access patterns to other AWS security services described in the preceding sections. Macie can send findings to AWS Security Hub to enable a consolidated view of security findings. Another essential feature that FRFIs can use for supporting data classification and protection is AWS resource tagging. Customers can manage, identify, organize, search, and filter resources by assigning metadata to their AWS resources (with each tag being a label consisting of a user-defined value and key). For example, security tags can contain information on confidentiality, identifying the specific data confidentiality levels a resource supports, or compliance, such as an identifier for workloads that must adhere to specific compliance requirements.	SEC03-BP07 Analyze public and cross-account access SEC04-BP02 Analyze logs, findings, and metrics centrally SEC05-BP04 Implement inspection and protection SEC06-BP02 Reduce attack surface SEC06-BP05 Enable people to perform actions at a distance SEC07-BP01 Identify the data within your workload SEC07-BP02 Define data protection controls SEC07-BP03 Automate identification and classification SEC07-BP04 Define data lifecycle management SEC09-BP03 Automate detection of unintended data access SEC10-BP02 Develop incident management plans REL06-BP01 Monitor all components for the workload (Generation)

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.1.5: FRFIs should maintain continuous situational awareness of the external cyber threat landscape and its threat environment as it applies to their technology assets. This could include participating in industry threat intelligence and information sharing forums and subscribing to timely and reputable threat information sources. Where feasible, FRFIs are encouraged to provide timely exchange of threat intelligence to facilitate prevention of cyber attacks, thereby contributing to their own cyber resilience and that of the broader financial sector.	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them: Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and anomalous behavior to protect AWS accounts, workloads, Kubernetes clusters, and data stored in Amazon S3. GuardDuty threat intelligence is provided by AWS and third-party providers, such as Proofpoint and CrowdStrike. These threat intelligence feeds are pre-integrated and continuously updated in GuardDuty at no additional cost. GuardDuty also allows customers to upload their threat intelligence data. The AWS Security Bulletins website provides customers with updated information on security and privacy events with AWS services. In addition, customers can subscribe to the AWS Security Bulletin RSS Feed to keep abreast of security announcements. Regarding exchanging intelligence to prevent cyberthreats, AWS customers can also report issues to AWS through the AWS Vulnerability Reporting website.	OPS01-BP05 Evaluate threat landscape SEC01-BP03 Identify and validate control objectives SEC01-BP04 Keep up-to-date with security threats SEC01-BP07 Identify threats and prioritize mitigations using a threat model SEC04-BP03 Automate response to events SEC04-BP04 Implement actionable security events SEC05-BP03 Automate network protection SEC05-BP04 Implement inspection and protection SEC06-BP01 Perform vulnerability management SEC11-BP01 Train for application security SEC11-BP08 Build a program that embeds security ownership in workload teams

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.1.6: Where feasible, FRFIs should maintain cyber threat models to identify cyber security threats directly facing their technology assets and services. Threats should be assessed regularly to enhance the cyber security program, capabilities and controls required to mitigate current and emerging threats. FRFIs should use manual techniques to proactively identify and isolate threats that might not be detected by automated tools (for example, threat hunting).	**Customer responsibility** This is an action for FRFIs to complete independently.	OPS01-BP05 Evaluate threat landscape SEC01-BP07 Identify threats and prioritize mitigations using a threat model
Section 3.1.7: FRFIs should enable and encourage their employees, customers and third parties to report suspicious cyber activity, recognizing the role that each can play in preventing cyber attacks. FRFIs should create awareness of cyber attack scenarios directly targeting employees, customers, and relevant third parties. In addition, the FRFI should regularly test its employees to assess their awareness of cyber threats and the effectiveness of their reporting processes and tools.	**Customer responsibility** This is an action for FRFIs to complete independently.	Not applicable.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.1.8: FRFIs should maintain, and report on, a current and comprehensive cyber security risk profile to facilitate oversight and timely decision making. The profile should draw on existing internal and external risk identification and assessment sources, processes, tools, and capabilities. FRFIs should also ensure that processes and tools exist to measure, monitor, and aggregate residual risks.	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them: AWS Security Hub is a cloud security posture management service that performs automated, continuous security best practice checks against customers' AWS resources. In addition, Security Hub aggregates security alerts (that is, findings) from various AWS services and partner products in a standardized format so that customers can take action more quickly.	SEC01-BP03 Identify and validate control objectives SEC02-BP05 Audit and rotate credentials periodically SEC04-BP04 Implement actionable security events SEC08-BP03 Automate data at rest protection SEC03-BP07 Analyze public and cross-account access SEC03-BP08 Share resources securely within your organization SEC04-BP01 Configure service and application logging SEC04-BP02 Analyze logs, findings, and metrics centrally SEC06-BP01 Perform vulnerability management SEC11-BP07 Regularly assess security properties of the pipelines

Purposely left blank.

Section 3.2 – Defend

Principle 15: FRFIs should design, implement, and maintain multi-layer, preventive cyber security controls and measures to safeguard their technology assets.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.2.1: FRFIs should adopt secure-by-design practices to safeguard their technology assets. Security defense controls should aim to be preventive, where feasible, and FRFIs should regularly review security use cases with a view to strengthen reliance on preventive as opposed to detective controls. Standard security controls should be applied end-to-end, starting at the design stage, to applications, micro-services, and application programming interfaces developed by the FRFI.	**Customer responsibility** This is an action for FRFIs to complete independently. AWS defines the most critical aspects of security in the cloud for customers through mechanisms such as the AWS Well-Architected Framework (which includes a specific Financial Services Industry Lens) and the AWS Cloud Adoption Framework. Both frameworks have specific security areas, including detailed whitepapers, that help focus on how to design and build secure cloud environments.	Not applicable.
Section 3.2.2: FRFIs should implement and maintain strong cryptographic technologies to protect the authenticity, confidentiality, and integrity of their technology assets. This includes controls for the protection of encryption keys from unauthorized access, usage, and disclosure throughout the cryptographic key management life cycle. FRFIs should regularly assess their cryptography standard and technologies to remain	**Customer responsibility** AWS customers might use AWS cryptographic services, which use a wide range of encryption and storage technologies to assure customer data's integrity at rest or in transit. In addition, AWS offers several tools for cryptographic operations: AWS Key Management Service (AWS KMS) is a managed service that makes it simple for customers to create and control the cryptographic keys that are used to protect their data. AWS KMS uses hardware security modules (HSM) to protect and validate customers' AWS KMS keys under the FIPS 140-2 Cryptographic Module Validation Program. AWS CloudHSM provides customers with dedicated HSMs within the AWS Cloud that can securely store various cryptographic keys.	SEC02-BP01 Use strong sign-in mechanisms SEC08-BP01 Implement secure key management SEC08-BP02 Enforce encryption at rest SEC08-BP04 Enforce access control SEC08-BP05 Use mechanisms to keep people away from data PERF04-BP01 Understand data characteristics

Requirements summary	Considerations for AWS customers	Well-Architected best practices
effective against current and emerging threats.	CloudHSM allows you to securely generate, store, and manage cryptographic keys used for data encryption. AWS Encryption SDK provides a client-side encryption library for implementing encryption and decryption operations on various data types. AWS Secrets Manager is a secrets management service that enables customers to quickly rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. AWS cryptographic services comply with a wide range of cryptographic security standards, helping customers to protect their data without worrying about governmental or professional regulations. For a complete list of AWS data security standard compliances, see AWS Compliance Programs.	REL10-BP04 Use bulkhead architectures to limit scope of impact
Section 3.2.3: FRFIs should employ enhanced controls and functionality to rapidly contain cyber security threats, defend their critical technology assets and remain resilient against cyber attacks by considering the following: • Identifying cyber security controls required to secure its critical technology assets; • Designing application controls to contain and limit the impact of a cyber attack;	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them: AWS Security Hub is a cloud security posture management service that provides customers with a comprehensive view of their security state within AWS and compliance with security standards and best practices. Security Hub supports multiple security standards that customers can enable. For example, the Payment Card Industry Data Security Standard (PCI DSS) in Security Hub provides AWS security best practices for handling cardholder data. In addition, these automated checks can assist FRFIs in preparing for a PCI DSS assessment. To run security checks on resources in the customer environment, Security Hub uses steps specified by the standard or specific AWS Config rules. AWS Config provides a detailed view of the configuration of AWS resources in an AWS account. This includes how the resources are	SEC04-BP01 Configure service and application logging SEC05-BP01 Create network layers SEC05-BP02 Control traffic at all layers SEC05-BP03 Automate network protection SEC05-BP04 Implement inspection and protection SEC06-BP02 Reduce attack surface SEC06-BP04 Automate compute protection

Requirements summary	Considerations for AWS customers	Well-Architected best practices
• Implementing, monitoring, and reviewing appropriate security standards, configuration baselines, and security hardening requirements; and • Deploying additional layers of security controls, as appropriate, to defend against cyber attacks (for example, volumetric, low/slow network and application business logic attacks).	related to one another and how they were configured in the past so that customers can see how the configurations and relationships change over time. AWS WAF is a web application firewall that helps protect customers' web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. With AWS WAF, customers can create security rules that control bot traffic and block common threat patterns such as SQL injection or cross-site scripting (XSS). AWS Shield is a managed service that protects against distributed denial of service (DDoS) attacks for applications running on AWS. AWS Shield Standard is automatically enabled for all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service.	SEC06-BP05 Enable people to perform actions at a distance SEC10-BP04 Automate containment capability PERF05-BP01 Understand how networking impacts performance
Section 3.2.4: FRFIs should implement and maintain multiple layers of cyber security controls and defend against cyber security threats at every stage of the attack life cycle (for example, from reconnaissance and initial access to executing on objectives). FRFIs should also ensure resilience against current and emerging cyber threats by maintaining defense controls and tools. This includes ensuring continuous operational effectiveness of controls by minimizing false positives. Where feasible, FRFIs should:	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them: The Amazon Virtual Private Cloud (Amazon VPC) lets customers provision a private, isolated section of the AWS Cloud where they can launch AWS services and other resources in a virtual network defined by them. Customers have complete control over their virtual networking environment, including selecting an IP address range, creating subnets, and configuring route tables and network gateways. Furthermore, customers can separate subnets for unique routing requirements. AWS recommends using public subnets for external-facing resources and private subnets for internal resources. Network ACLs (NACL) can be used as firewalls to control inbound and outbound traffic at the subnet level. In addition, the security group controls the traffic that's allowed to reach and leave the resources that it's associated with. A security group is a virtual firewall that controls	SEC04-BP01 Configure service and application logging SEC05-BP01 Create network layers SEC05-BP02 Control traffic at all layers SEC05-BP03 Automate network protection SEC05-BP04 Implement inspection and protection SEC06-BP02 Reduce attack surface SEC06-BP04 Automate compute protection

Requirements summary	Considerations for AWS customers	Well-Architected best practices
• Protect networks, including external-facing services, from threats by minimizing their attack surface; • Define authorized logical network zones and apply controls to segregate and limit, or block access and traffic to and from network zones; • Leverage a combination of allow/deny lists, including file integrity checks (for example, file hash/signature) and indicators of compromise, in addition to advanced behavior-based protection capabilities that are continuously updated; and • Apply defense controls and capabilities for intrusion prevention and detection on its network perimeter in addition to controls for data loss, malware, and viruses.	inbound and outbound traffic to your network resources and EC2 instance. AWS WAF is a web application firewall that helps protect customers' web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives customers control over which traffic to allow or block to their web applications by defining customizable web security rules. Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and anomalous behavior to protect customers' AWS accounts, workloads, Kubernetes clusters, and data stored in Amazon S3. GuardDuty service monitors for unusual API calls, unauthorized deployments, and exfiltrated credentials that indicate a possible account reconnaissance or compromise. GuardDuty Malware Protection is an enhancement to GuardDuty. GuardDuty identifies resources that have already been compromised by malware or those at risk. Malware Protection supports GuardDuty to detect the malware that might be the source of this compromise. AWS Network Firewall is a high-availability, managed network firewall service for VPCs. It enables customers to quickly deploy and manage stateful inspection, intrusion prevention and detection, and web filtering to help protect customers' virtual networks on AWS. In addition, the network Firewall automatically scales with traffic, ensuring high availability with no additional customer investment in security infrastructure.	SEC06-BP05 Enable people to perform actions at a distance SEC10-BP04 Automate containment capability PERF05-BP01 Understand how networking impacts performance
Section 3.2.5: Starting with clear information classification of its data, FRFIs should design and implement risk-based controls for the protection of	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them:	SEC03-BP07 Analyze public and cross-account access

Requirements summary	Considerations for AWS customers	Well-Architected best practices
their data throughout its life cycle. This includes data loss prevention capabilities and controls for data at rest, data in transit and data in use.	Amazon Macie is a data security service that discovers sensitive data using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks. Using AWS Identity and Access Management (IAM), customers can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources. See Section 3.2.2 for AWS cryptographic services, which customers can use to protect their data at rest or in transit.	SEC04-BP02 Analyze logs, findings, and metrics centrally SEC05-BP04 Implement inspection and protection SEC06-BP02 Reduce attack surface SEC06-BP05 Enable people to perform actions at a distance SEC07-BP01 Identify the data within your workload SEC07-BP02 Define data protection controls SEC07-BP03 Automate identification and classification SEC07-BP04 Define data lifecycle management SEC09-BP03 Automate detection of unintended data access SEC10-BP02 Develop incident management plans
Section 3.2.6: To ensure security vulnerabilities are well managed, FRFIs should:	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them: Amazon Inspector is a vulnerability management service that continuously scans AWS workloads for software vulnerabilities and	SEC04-BP02 Analyze logs, findings, and metrics centrally SEC05-BP01 Create network layers

Requirements summary	Considerations for AWS customers	Well-Architected best practices
• Maintain capabilities to ensure timely risk-based patching of vulnerabilities, in vendor software and internal applications, that considers the severity of the threat and vulnerability of the exposed systems; • Apply patches at the earliest opportunity, commensurate with risk and in accordance with established timelines; • Implement compensating controls as needed to sufficiently mitigate risks when remediation options are not available (for example, "zero-day" attacks); and • Regularly monitor and report on patching status and vulnerability remediation against defined timelines, including any backlog and exceptions.	unintended network exposure. As Amazon Inspector collects information about a customer's environment through scans, it provides severity scores tailored to that environment. Customers can use the Amazon Inspector risk score to prioritize remediation actions efficiently. Customers can perform regular patching operations for resolving vulnerabilities identified by Amazon Inspector by using AWS Systems Manager Patch Manager to automate the process of patching nodes. Customers can also use Systems Manager Automation Runbooks to perform on-demand remediation of vulnerability findings.	SEC05-BP03 Automate network protection SEC05-BP04 Implement inspection and protection SEC06-BP01 Perform vulnerability management SEC06-BP02 Reduce attack surface SEC07-BP03 Automate identification and classification SEC09-BP03 Automate detection of unintended data access

Section 3.2.7: FRFIs should implement risk-based identity and access controls, including multi-factor authentication (MFA) and privileged access management. Where feasible, FRFIs should consider: • Enforcing the principles of least privilege, conducting regular attestation of access and maintaining strong complex passwords to authenticate employee, customer, and third-party access to technology assets; • Implementing MFA across external-facing channels and privileged accounts (for example, customers, employees, and third parties); • Managing privileged account credentials using a secure vault; • Logging and monitoring account activity as part of continuous security monitoring; • Ensuring system and service accounts are securely authenticated, managed, and monitored to detect unauthorized use; and	**Customer responsibility** Using AWS Identity and Access Management (IAM), AWS customers can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources. Customers can set a custom password policy on their AWS account to specify complexity requirements and mandatory rotation periods for their IAM users' passwords. If a custom password policy is not set, IAM user passwords must meet the default AWS password policy. IAM Access Analyzer helps customers analyze access across their AWS environments and provides features such as policy generation and policy validation to help customers achieve the least privilege access. AWS customers can also use AWS IAM Identity Center to create or connect workforce identities in AWS once and manage access centrally to multiple AWS accounts, AWS applications, and other SAML-enabled cloud applications. Customers can create users directly in IAM Identity Center or from an existing workforce directory. IAM Identity Center also integrates with AWS Security partner offerings to provide customers with a choice of solutions for temporary elevated access in different business and technical environments. AWS Multi-factor Authentication (MFA) for highly privileged users is a security feature that augments username and password credentials. MFA requires users to prove physical possession of a hardware MFA token or MFA-enabled mobile device by providing a valid MFA code. Customers can enable MFA at the AWS account level and for root and IAM users they have created in their account. AWS CloudTrail enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage. CloudTrail logs continuously monitor and retain account activity related to actions across a customer's AWS infrastructure, giving them control over storage, analysis, and remediation actions.	SEC02-BP02 Use temporary credentials SEC02-BP04 Rely on a centralized identity provider SEC02-BP05 Audit and rotate credentials periodically SEC02-BP06 Leverage user groups and attributes SEC03-BP01 Define access requirements SEC03-BP02 Grant least privilege access SEC03-BP03 Establish emergency access process SEC03-BP04 Reduce permissions continuously SEC03-BP05 Define permission guardrails for your organization SEC03-BP07 Analyze public and cross-account access

• Performing appropriate background checks (where feasible) on persons granted access to the FRFI's systems or data, commensurate with the criticality and classification of the technology assets.		
Section 3.2.8: FRFIs should implement approved, risk-based security configuration baselines for technology assets and security defense tools, including those provided by third parties. Where possible, security configuration baselines for different defense layers should disable settings and access by default. FRFIs should define and implement processes to manage configuration deviations.	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them: EC2 Image Builder simplifies creating, maintaining, validating, sharing, and deploying Linux or Windows images for use with Amazon EC2 and on-premises. Image Builder allows customers to define collections of security settings that they can use to harden their images built using Image Builder. These settings collections can be applied toward meeting applicable compliance criteria. AWS provides a gallery of settings to help meet industry regulations. AWS Service Catalog enables organizations to create and manage catalogues of IT services that are approved for AWS. These IT services can include everything from virtual machine images, servers, software, databases, and more to complete multi-tier application architectures. Customers can administer and manage approved assets by restricting where the product can be launched, the type of instance that can be used, and many other configuration options. The result is a standardized landscape for product provisioning for the entire organization. AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations. As new applications are created, Firewall Manager makes it easy to bring new applications	OPS05-BP05 Perform patch management OPS05-BP06 Share design standards OPS09-BP03 Collect and analyze operations metrics REL10-BP01 Deploy the workload to multiple locations SEC06-BP02 Reduce attack surface SEC11-BP01 Train for application security COST11-BP01 Perform automations for operations SUS06-BP02 Keep your workload up-to-date

	and resources into compliance by enforcing a common set of security rules. AWS Config provides a detailed view of the configuration of AWS resources in an AWS account. This includes how the resources are related to one another and how they were configured in the past so that customers can see how the configurations and relationships change over time.	
Section 3.2.9: Where feasible, static and/or dynamic scanning and testing capabilities should be used to ensure new, and/or changes to existing, systems and applications are assessed for vulnerabilities prior to release into the production environment. Security controls should also be implemented to maintain security when development and operations practices are combined through a continuous and automated development pipeline (see paragraph 2.4.2).	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them: Amazon Inspector is a vulnerability management service that continuously scans AWS workloads for software vulnerabilities and unintended network exposure. Amazon Inspector automatically discovers and scans running Amazon EC2 instances, container images in Amazon Elastic Container Registry (Amazon ECR), and AWS Lambda functions for known software vulnerabilities and unintended network exposure. Customers can also integrate Amazon Inspector in their CI/CD pipelines by using other AWS services. For example, the pipeline build stage creates a container image and pushes it to Amazon ECR. Then, Amazon Inspector scans the image for vulnerabilities. Finally, the Lambda function receives the Amazon Inspector scan summary message through Amazon EventBridge, allowing the image to be deployed.	SEC04-BP02 Analyze logs, findings, and metrics centrally SEC05-BP01 Create network layers SEC05-BP03 Automate network protection SEC05-BP04 Implement inspection and protection SEC06-BP01 Perform vulnerability management SEC06-BP02 Reduce attack surface SEC11-BP02 Automate testing throughout the development and release lifecycle
Section 3.2.10: FRFIs should define and implement physical access management controls and processes to protect network infrastructure and other technology assets from	**AWS responsibility** AWS has implemented a formal, documented physical and environmental protection policy that is updated and reviewed annually.	Not applicable.

unauthorized access and environmental hazards.	Physical access to AWS data centers housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access to perform their jobs. Access to facilities is only permitted at controlled access points requiring multi-factor authentication designed to prevent tailgating and make sure that only authorized individuals enter an AWS data center. Quarterly access lists and authorization credentials of personnel with access to data centers housing systems and devices within the system boundary are reviewed by the respective data center Area Access Managers (AAM). Entrances to AWS data centers, including the main entrance, the loading dock, and roof doors and hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. Trained security guards are stationed at the building entrance 24/7. In addition, if a door or cage within a data center has a malfunctioning card reader or PIN pad and cannot be secured electronically, a security guard is posted at the door until it can be repaired. See Data Center Controls.	

Section 3.3 – Detect

Principle 16: FRFIs design, implement and maintain continuous security detection capabilities to enable monitoring, alerting, and forensic investigations.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.3.1: FRFIs should ensure continuous security logging for technology assets and different layers of defense tools. Central tools for aggregating, correlating, and managing security event logs should enable timely log access during a cyber event	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them: AWS CloudTrail enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage. CloudTrail logs continuously monitor and retain account activity related to actions across	OPS04-BP02 Implement and configure workload telemetry OPS11-BP05 Define drivers for improvement

Requirements summary	Considerations for AWS customers	Well-Architected best practices
investigation. For any significant cyber threat or incident, the FRFI's forensic investigation should not be limited or delayed by disaggregated, inaccessible, or missing critical security event logs. FRFIs should implement minimum security log retention periods and maintain cyber security event logs to facilitate a thorough and unimpeded forensic investigation of cyber security events.	customers' AWS infrastructure, giving them control over storage, analysis, and remediation actions. Amazon Security Lake is a service that automates the sourcing, aggregation, normalization, and data management of security data across customers' organizations into a security data lake stored in their accounts. A security data lake helps make the organization's security data broadly accessible to their preferred security analytics solutions to power use cases such as threat detection, investigation, and incident response. Amazon Detective helps customers analyze, investigate, and quickly identify the root cause of security findings or suspicious activities. Detective automatically collects log data from AWS resources. It then uses machine learning, statistical analysis, and graph theory to generate visualizations that help customers to conduct faster and more efficient security investigations.	REL06-BP06 Conduct reviews regularly SEC04-BP01 Configure service and application logging SEC04-BP02 Analyze logs, findings, and metrics centrally SEC10-BP04 Automate containment capability
Section 3.3.2: FRFIs should maintain security information and event management capabilities to ensure continuous detection and alerting of malicious and unauthorized user and system activity. Where feasible, advanced behavior-based detection and prevention methods should be used to detect user and entity behavior anomalies and emerging external and internal threats. The latest threat intelligence and indicators of compromise should be used to continuously enhance FRFI monitoring tools.	**Customer responsibility** AWS customers might use the following AWS services and resources to assist them in addition to the services mentioned in section 3.3.1: Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and anomalous behavior to protect your AWS accounts, workloads, Kubernetes clusters, and data stored in Amazon S3. GuardDuty looks for atypical API requests, unapproved deployments, and access credentials that might suggest a potential account reconnaissance or breach.	OPS07-BP01 Ensure personnel capability OPS11-BP04 Perform knowledge management SEC03-BP01 Define access requirements SEC03-BP04 Reduce permissions continuously SEC03-BP06 Manage access based on lifecycle

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.3.3: FRFIs should define roles and responsibilities to allow for the triage of high-risk cyber security alerts to rapidly contain and mitigate significant cyber threat events before they result in a material security incident or an operational disruption.	**Customer responsibility** This is an action for FRFIs to complete independently. AWS customers might use the following AWS services and resources to assist them: The AWS Security Incident Response Guide presents an overview of the fundamentals of responding to security incidents within a customer's AWS Cloud environment. It focuses on an overview of cloud security and incident response concepts and identifies cloud capabilities, services, and mechanisms available to customers responding to security issues.	SEC10-BP01 Identify key personnel and external resources SEC10-BP02 Develop incident management plans

Purposely left blank.

Section 3.4 – Respond, Recover and Learn

Principle 17: FRFIs should respond to, contain, recover, and learn from cyber security incidents impacting their technology assets, including incidents originating at third-party providers.

Requirements summary	Considerations for AWS customers	Well-Architected best practices
Section 3.4.1: Domain 2 sets out the foundational expectations for FRFIs' incident and problem management capabilities. FRFIs should ensure the alignment and integration between their cyber security, technology, crisis management, and communication protocols. This should include capabilities to enable comprehensive and timely escalation and stakeholder coordination (internal and external) in response to a major cyber security event or incident.	**Customer responsibility** This is an action for FRFIs to complete independently. AWS customers might use the following AWS services and resources to assist them: AWS Systems Manager Incident Manager is an incident management console designed to help users mitigate and recover from incidents affecting their AWS-hosted applications. An incident is any unplanned interruption or reduction in the quality of services. Incident Manager increases incident resolution by notifying responders of impact, highlighting relevant troubleshooting data, and providing collaboration tools to get services back up and running. In addition, to achieve the primary goal of reducing the time-to-resolution of critical incidents, Incident Manager automates response plans and enables responder team escalation.	OPS10-BP01 Use a process for event, incident, and problem management SEC10-BP02 Develop incident management plans
Section 3.4.2: FRFIs should clearly define and implement a cyber incident taxonomy. This taxonomy should include specific cyber and information security incident classification, such as severity, category, type, and root cause. It should be designed to support the FRFI in responding to, managing, and reporting on cyber security incidents.	**Customer responsibility** This is an action for FRFIs to complete independently.	Not applicable.
Section 3.4.3: FRFIs should maintain a cyber security incident management process and playbooks to enable timely	**Customer responsibility** This is an action for FRFIs to complete independently.	SEC10-BP02 Develop incident management plans

Requirements summary	Considerations for AWS customers	Well-Architected best practices
and effective management of cyber security incidents.	To support our customer's creation of incident management processes and security playbooks, AWS is providing the AWS Customer Playbook Framework. This publicly available response framework uses AWS customer incident response team (CIRT) lessons learned from security events. This collection of files is provided as an example framework for customers to create, develop, and integrate security playbooks in preparation for potential attack scenarios when using AWS services.	OPS07-BP04 Use playbooks to investigate issues OPS10-BP01 Use a process for event, incident, and problem management
Section 3.4.4: FRFIs should establish a cyber incident response team with tools and capabilities available on a continuous basis to rapidly respond, contain, and recover from cyber security events and incidents that could materially impact the FRFI's technology assets, customers, and other stakeholders.	**Customer responsibility** This is an action for FRFIs to complete independently. AWS customers can engage the AWS customer incident response team (CIRT) through a support case to assist with triage and recovery for an active security event on AWS. The AWS CIRT is a specialized 24/7 global AWS team that provides support to customers during active security events on the customer side of the AWS Shared Responsibility Model. The team is made up of AWS Global Services Consultants and Solutions Architects with experience in incident response. When engaged, the AWS CIRT assists in root cause analysis through AWS service logs and provides customers with recommendations for recovery. In addition, the AWS CIRT provides security tips and best practices to help customers avoid security events in the future.	OPS10-BP01 Use a process for event, incident, and problem management OPS11-BP02 Perform post-incident analysis SEC10-BP07 Run game days
Section 3.4.5: FRFIs should conduct a forensic investigation for incidents where technology assets might have been materially exposed. For high-severity incidents, the FRFI should conduct a detailed post-incident assessment of direct and indirect impacts (financial and/or non-financial), including a root cause analysis to identify remediation actions, address	**Customer responsibility** This is an action for FRFIs to complete independently. AWS offers a wide range of security capabilities that customers can use to investigate security events across the domains, which include some logging mechanisms, such as AWS CloudTrail logs, Amazon CloudWatch Logs, Amazon S3 access logs, and more. Amazon Security Lake is a service that automates the sourcing, aggregation, normalization, and data management of security data across customers' organizations into a security data lake stored in their accounts. A security data	SEC04-BP04 Implement actionable security events SEC10-BP02 Develop incident management plans SEC10-BP03 Prepare forensic capabilities

Requirements summary	Considerations for AWS customers	Well-Architected best practices
the root cause, and respond to lessons learned. The root cause analysis should assess threats, weaknesses, and vulnerabilities in its people, processes, technology, and data.	lake helps make an organization's security data broadly accessible to their preferred security analytics solutions to power use cases such as threat detection, investigation, and incident response. Several AWS services can help customers get valuable insights into this data, such as Amazon GuardDuty (a threat detection service) and AWS Security Hub, which can give customers a comprehensive view of their high-priority security alerts and compliance status across AWS accounts. Additionally, Amazon Detective collects log data from customers' AWS resources and uses machine learning, statistical analysis, and graph theory to help them identify the root cause of potential security issues or suspicious activities.	OPS07-BP04 Use playbooks to investigate issues

Document revisions

Date	Description
March 2024	First publication