AWS User Guide to Risk Management in Technology

Bank Negara Malaysia – Central Bank of Malaysia

March 2026



Notices

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

Additionally, this document does not constitute legal advice and should not be relied on as legal advice. AWS encourages its customers to obtain appropriate advice on their implementation of privacy and data protection environments, and more generally, applicable laws relevant to their business.

© 2026 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

Introduction 1

Security and the AWS Shared Responsibility Model 2

AWS Compliance programs 4

AWS Global Cloud Infrastructure 6

Getting started 7

Further reading 8

Appendix 1: AWS considerations on Risk Management in Technology 10

- Technology Project Management 11
- System Development and Acquisition 13
- Patch and End-of-Life System Management 16
- Cryptography 18
- Data Centre Resilience 21
- Service Availability 24
- Network Resilience 28
- System backup and restoration 31
- Third Party Service Provider Management 33
- Cloud Services 35
- Access Control 37
- Cyber Risk Management 39
- Cybersecurity Operations 41
- Cyber Response and Recovery 44
- Cyber Reporting and Threat Information Sharing 46

Document revisions 48

Abstract

This document provides AWS customers in Malaysia's financial services sector with comprehensive guidance on leveraging AWS cloud services to help meet Bank Negara Malaysia's Risk Management in Technology (RMiT) regulatory requirements. It serves as a practical reference for financial institutions navigating cloud adoption within Malaysia's regulatory framework.

The guide is structured around the AWS Shared Responsibility Model, clearly delineating security responsibilities between AWS (security of the cloud) and customers (security in the cloud). AWS maintains the underlying infrastructure, including physical security, hardware, networking, and facilities, while customers retain control over their data, applications, access management, and security configurations.

Key areas covered include technology project management, system development lifecycle, patch management, cryptography, data center resilience, service availability, network resilience, backup and restoration, third-party service provider management, cloud services adoption, access control, cyber risk management, cybersecurity operations, incident response and recovery, and cyber reporting obligations.

For each RMiT requirement, the document provides AWS considerations explaining how the shared responsibility model applies, relevant AWS services and features that support compliance efforts, and specific best practices from the AWS Well-Architected Framework. The six pillars of this framework—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability—form the foundation for implementing secure and compliant cloud architectures.

The guide emphasizes that financial institutions remain accountable for regulatory compliance and must conduct appropriate due diligence, risk assessments, and implement controls suitable to their risk profile. AWS provides the infrastructure, services, tools, and compliance certifications (including ISO 27001, SOC reports, and PCI DSS) to support customers' compliance journeys, with detailed audit reports accessible through AWS Artifact. This document enables financial institutions to make informed decisions about cloud adoption while maintaining robust governance, security, and operational resilience.

Introduction

Bank Negara Malaysia has issued comprehensive guidelines to help financial institutions navigate the complex landscape of technology and cyber risks. These requirements, effective November 28, 2025, recognize that as financial services become increasingly digital, institutions must invest deeply in security controls and operational resilience to maintain public confidence.

The policy establishes clear accountability at the highest levels. Boards must approve technology risk appetites and oversee strategic IT plans, while a designated Chief Information Security Officer ensures day-to-day protection of information assets. Financial institutions need robust frameworks covering everything from system development and cloud services to cybersecurity operations and incident response. The guidance emphasizes practical measures like multi-factor authentication for digital transactions, real-time fraud detection, and tamper-proof backup arrangements to enable swift recovery from cyberattacks.

Special attention goes to managing third-party service providers, particularly for cloud services and critical systems. Institutions must conduct thorough due diligence, maintain clear service agreements, and ensure continuous monitoring of provider performance. The policy also requires regular testing through penetration exercises and cyber drills, ensuring teams stay prepared for evolving threats.

Security and the AWS Shared Responsibility Model

Cloud security is a shared responsibility and financial institutions need to understand the AWS Shared Responsibility Model before reviewing their operational and technical requirements under BNM's Risk Management in Technology (RMiT). AWS manages the security of the cloud by maintaining the AWS Cloud Infrastructure aligned with global and regional regulatory requirements and best practices. Security in the cloud is the responsibility of the AWS customer. Namely, our customers retain control of the security programs that they choose to implement to protect their content, applications, systems, and networks, because they are responsible for applications in an on-premises data center.

AWS customers must carefully consider the services they choose because their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides flexibility and customer control to workloads. As shown in Figure 1, this differentiation of responsibility is commonly referred to as security *of* the cloud versus security *in* the cloud.

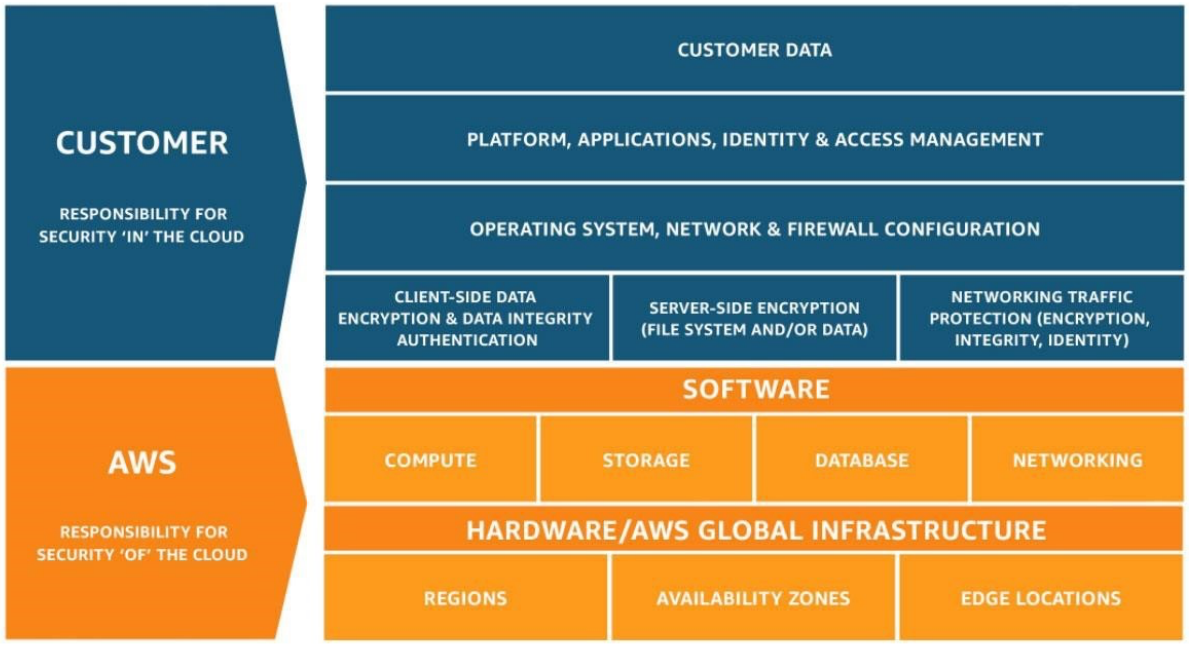


Figure 1 – The AWS Shared Responsibility Model

AWS responsibility - security of the Cloud: AWS is responsible for protecting the infrastructure that runs the AWS services. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS services.

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

For abstracted 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. 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.

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.

The AWS Shared Responsibility Model also extends to IT controls. The responsibility to operate the IT environment is shared between AWS and its customers, and so is the responsibility for the management, operation, and verification of IT controls. AWS can reduce the administrative load on customers by managing the controls associated with

the physical infrastructure deployed in the AWS environment that might previously have been managed by the customer.

AWS Compliance programs

AWS has obtained certifications and independent third-party attestations for a variety of industry-specific workloads. The following compliance programs might be of particular importance to financial institutions:

- **ISO 27001**: A security management standard that specifies security management best practices and comprehensive security controls that follow the ISO 27002 best practice guidance. For more information or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.
- **ISO 27017**: Provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. For more information or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.
- **ISO 27018**: Code of practice that focuses on protecting personal data in the cloud. It is based on the ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls that are applicable to cloud personally identifiable information (PII). For more information or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.
- **ISO 27701** Specifies requirements and guidelines to establish and continuously improve the Privacy Information Management System (PIMS), including processing of Personally Identifiable Information (PII). For more information, or to download the AWS ISO 27701 certification, see the ISO 27701 Compliance webpage.
- **ISO 22301**: Specifies the structure and requirements to implement, maintain, and improve a business continuity management system (BCMS) to protect against, reduce the likelihood of the occurrence of, prepare for, respond to, and recover from disruptions when they arise. Compliance to this standard provides assurance on AWS commitment to business continuity and resiliency of AWS services. For more information or to download the AWS ISO 22301 certification, see the ISO 22301 Compliance webpage.

- **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. 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.

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, AWS Artifact is designed to provide 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.

Support plans

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

Basic Support is included for all AWS customers and includes:

- Customer Service and Communities offer 24x7 access to customer service, documentation, whitepapers, and support forums.
- AWS Trusted Advisor is designed to provide seven core Trusted Advisor checks and guidance to provision resources following best practices to increase performance and improve security.
- AWS Personal Health Dashboard is designed to provide a personalized view of the health of AWS services, and alerts when customer resources are impacted.

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, which are more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment.

AWS customers choose the Region where their content and applications are located. Regions allow AWS customers to establish environments that meet geographic or regulatory requirements. Additionally, Regions allow AWS customers with business continuity and disaster recovery objectives to establish primary and backup environments in locations of their choice. More information is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

The AWS Malaysia Region consists of three Availability Zones, giving customers more choice and flexibility to leverage advanced technologies from AWS. The addition of the Region in 2024 is a natural progression of our investment and support of our customers The Malaysia Region will also enable customers with data residency preferences to store data securely in Malaysia, help customers to achieve even lower latency, and serve demand for cloud services across Asia. For more information see the AWS Malaysia Region page.

Getting started

Each organization's cloud adoption journey is unique; and so, financial institutions need to understand their current state, the desired target state, and the transition required to achieve the target state to manage the cloud adoption successfully. Knowing this helps set goals and create work streams that enable staff to thrive in the cloud.

For financial institutions Malaysia, the next steps are:

- Contact your AWS representative to discuss how the AWS Partner Network, and AWS Solution Architects, Professional Services teams, and training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, contact us.
- Obtain and review a copy of the latest AWS SOC 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification from AWS Artifact that is accessible through the AWS Management Console.
- Consider the relevance and application of the AWS security whitepapers, AWS Well-Architected Framework, and the CIS Amazon Web Services Foundations Benchmark, as appropriate for your cloud journey and use cases. These industry-accepted best practices, provide AWS customers with clear, step-by-step implementation and assessment recommendations.
- Explore other governance and risk management practices as necessary, do due diligence and risk assessment, using the tools and resources referenced throughout this guide.
- Contact your AWS representative to obtain additional information regarding the AWS Enterprise Agreement and determine the support level that matches your needs.

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

Further reading

The following resources can help financial institutions think about security and compliance when designing a secure and resilient environment on AWS.

- AWS Security & Compliance Quick Reference Guide AWS has many features to assist in aligning with compliance objectives for regulated workloads on AWS. These features can help achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry, simpler operations, and improved agility by providing more oversight, security control, and central automation.
- 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 AWS Security Documentation.
- The AWS Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures and provides guidance to help implement designs that scale application needs over time. The AWS Well-Architected Framework consists of six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability.
- AWS whitepapers on the six pillars of the AWS Well-Architected Framework: Operational Excellence Pillar; Security Pillar; Reliability Pillar; Performance Efficiency Pillar; Cost Optimization Pillar, and the Sustainability Pillar.
- Global Financial Services Regulatory Principles: AWS has identified five common principles related to financial services regulation that customers can consider when using AWS services and specifically, applying the Shared Responsibility Model to their regulatory requirements. AWS customers can review these principles on AWS Artifact.

- NIST Cybersecurity Framework (CSF): The AWS whitepaper NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud demonstrates how public and commercial sector organizations can assess the AWS environment against the NIST CSF and improve the security measures they implement and operate (that is, security in the cloud). The whitepaper also provides a third-party auditor letter attesting to the conformance to NIST CSF risk management practices (that is, security of the cloud) of AWS offerings. Financial institutions can use NIST CSF and AWS resources to support their risk management frameworks.

For more information, refer to the Security Learning whitepapers.

Appendix 1: AWS considerations on Risk Management in Technology

The following sections list key technical and operational requirements identified in Bank Negara Malaysia's Risk Management in Technology (RMiT) along with AWS considerations to assist financial institution customers in understanding each requirement when using AWS, and a description of the best practices from the AWS Well-Architected Framework, which financial institutions can use to support their compliance efforts.

The AWS Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on six pillars—Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)—the AWS Well-Architected Framework provides a consistent approach for customers to evaluate architectures and implement designs that scale over time.

The table is organized into the following columns:

- **Summary of requirements:** Summarizes the requirements identified in RMiT. This is not the original text of RMiT, but a summary.
- **AWS Considerations:** Explains the considerations for addressing the requirements identified in RMiT. It refers to security and compliance of the cloud, how AWS implements and manages controls, and AWS services that financial institution customers can use to address requirements.
- **Implementation:** Lists best practices for security in the cloud from the AWS Well-Architected Framework that financial institutions can implement as a starting point to support their compliance efforts. Details on each best practice and associated AWS services is available in the AWS Well-Architected Framework.

Technology Project Management

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.1 Financial institutions must establish governance requirements proportionate to technology project risk and complexity, including oversight roles, responsibilities, authority structures, reporting mechanisms, and risk assessments throughout the project life cycle. **S 10.2** Risk assessments must identify and address key implementation risks and potential broader operational impacts, with minimum consideration for: **(a)** adequacy and competency of resources (including vendor resources), considering concurrent significant projects; **(b)** system complexity including unproven technology, integration challenges, multi-vendor technologies, data migration, and customization; **(c)** security controls throughout project life cycle to prevent cybersecurity breaches and data exposure; (**d)** comprehensive user requirements to mitigate scope changes and business need deficiencies; **(e)** robust testing strategies to reduce undiscovered faults and errors; **(f)** appropriate deployment and fallback strategies to mitigate stability issues; and **(g)** adequate disaster recovery readiness post-implementation. **S 10.3** Board and senior management must receive and review timely ongoing risk management reports throughout significant project implementations.	**Customer responsibility** - Defining their governance, risk assessment, and operational process models - Project Risk Management - Governance and Reporting *AWS services and resources that can help support this requirement:* **AWS Well-Architected Framework** - Provides a consistent approach to evaluate architectures and implement scalable designs around six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability.	**OPS 2**: How do you structure your organization to support your business outcomes? **OPS 6**: How do you mitigate deployment risks? **OPS 7**: How do you know that you are ready to support a workload? **SEC 11**: How do you incorporate and validate security properties of apps during design, development, and deployment lifecycle? **REL 8**: How do you implement change? **REL 12**: How do you test reliability? **REL 13**: How do you plan for disaster recovery (DR)? **OPS 1**: How do you determine what your priorities are? **OPS 3**: How does your organizational culture support your business outcomes? **OPS 5**: How do you reduce defects, ease remediation, and improve flow into production? **OPS 10**: How do you manage workload and operations events? **REL 4**: How do you design interactions in a distributed system to prevent failures?

Summary of requirements	AWS Considerations	Implementation
		REL 5: How do you design interactions in a distributed system to mitigate or withstand failures?

System Development and Acquisition

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.4 Financial institutions must establish a framework for enterprise technology architecture that: **(a)** Provides comprehensive technology view and baseline components **(b)** Describes technical design, infrastructure, system connectivity, dependencies, and security controls **(c)** Maps business functions, units, applications, and data for impact analysis **(d)** Defines principles for network infrastructure design and IT security policies **(e)** Outlines long-term evolution priorities **S 10.5** Financial institutions must adopt SDLC methodology (requirement, design, development, testing, deployment, change management, maintenance, decommissioning) integrated with: **(a)** Enterprise architecture for business strategy execution **(b)** Risk management policies **(c)** Security principles for data confidentiality, integrity, and availability **S 10.6** Financial institutions using rapid development methodology must meet security, governance, and compliance requirements through automated IT security compliance reviews and vulnerability testing. **S 10.7** Production environments must be physically segregated from development/testing environments; cloud environments must not share virtual hosts. **S 10.8** Financial institutions must establish rigorous system testing methodology before deployment, with proper authorization and security measures for sensitive test data.	**Customer responsibility** - Enterprise Architecture Framework (S 10.4) - System Development Life Cycle (S 10.5, S 10.6) - Environment Segregation (S 10.7) - System Testing (S 10.8, G 10.9) - Source Code Reviews (S 10.10) - Change Management (S 10.11) - Third-Party Management (S 10.12) - System Decommissioning (S 10.13) - Software Security (G 10.15) - Shadow IT Management (S 10.16) *AWS services and resources that can help support this requirement:* *Architecture and Design (S 10.4)* **AWS Well-Architected Framework** – Provides a consistent approach to evaluate architectures and implement scalable designs across six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability **AWS Control Tower** – Provides governance and compliance for multi-account AWS environments **AWS Organizations** – Centrally manage and govern multiple AWS accounts *Development and Deployment (S 10.5, S 10.6, G 10.14)* **AWS CodePipeline** – Automates build, test, and deploy phases of the release process **AWS CodeBuild** – Compiles source code, runs tests, and produces software packages **AWS CodeDeploy** – Automates software deployments **AWS CodeCommit** – Secure Git-based repositories for source code version control **AWS CodeArtifact** – Artifact repository for software package management *Environment Segregation (S 10.7)* **AWS Organizations** – Create separate accounts for production, development, and testing	**SEC 11**: How do you incorporate and validate security properties of apps during design, development, and deployment lifecycle? **OPS 5**: How do you reduce defects, ease remediation, and improve flow into production? **OPS 6**: How do you mitigate deployment risks? **REL 8**: How do you implement change? **OPS 7**: How do you know that you are ready to support a workload? **OPS 1**: How do you determine what your priorities are? **OPS 2**: How do you structure your organization to support your business outcomes? **SEC 1**: How do you securely operate your workload? **SEC 6**: How do you protect your compute resources? **REL 12**: How do you test reliability?

Summary of requirements	AWS Considerations	Implementation
G 10.9 System testing scope may include unit, integration, user acceptance, security, stress/load, regression, exception, and negative testing. **S 10.10** Source code changes to critical systems require adequate security reviews before implementation. **S 10.11** Financial institutions must establish procedures for independent review/approval of system changes and test contingency plans for material changes. **S 10.12** For third-party developed/maintained critical systems, financial institutions must contractually require: **(a)** Sufficient notice before changes **(b)** Secure by design principles **(c)** Accessible source code for business continuity **S 10.13** System decommissioning must minimize customer and business impact, including tested contingency plans. **G 10.14** Financial institutions may deploy automated tools for development, testing, deployment, change management, and security assessment. **G 10.15** For third-party software, financial institutions should consider: **(a)** Adopting SBOM for vulnerability monitoring **(b)** Establishing open-source software security policies **S 10.16** Financial institutions must implement policies to identify and reduce shadow IT risks.	**Amazon VPC** – Isolated virtual networks for different environments **AWS Control Tower** – Automated multi-account setup with guardrails **AWS Resource Groups** – Organize and manage resources by environment *Testing and Quality Assurance (S 10.8, G 10.9)* **AWS Device Farm** – Application testing service for mobile and web applications **AWS CodeBuild** – Run automated tests as part of the CI/CD pipeline **AWS CloudFormation** – Infrastructure as code for consistent test environment provisioning **Amazon Macie** – Discover and protect sensitive test data *Security and Code Review (S 10.10)* **Amazon CodeGuru** – Automated code reviews and application performance recommendations **AWS CodePipeline** – Integrate security scanning into the deployment pipeline **Amazon Inspector** – Automated security assessment service **AWS Security Hub** – Centralized security and compliance view *Change Management (S 10.11)* **AWS Config** – Track resource configurations and changes **AWS CloudTrail** – Log and monitor account activity **AWS Systems Manager Change Manager** – Request, approve, implement, and report on operational changes **AWS Backup** – Centralized backup service for contingency planning *Monitoring and Compliance (S 10.6, G 10.14)* **AWS Security Hub** – Automated security checks and compliance monitoring **AWS Config Rules** – Evaluate resource configurations against desired configurations **Amazon GuardDuty** – Threat detection service **AWS Audit Manager** – Continuously audit AWS usage to simplify risk assessment *Software Composition Analysis (G 10.15)* **Amazon Inspector** – Automated vulnerability management for software dependencies **AWS Systems Manager** – Patch management and compliance scanning **Amazon ECR Image Scanning** – Scan container images for software vulnerabilities **AWS Security Hub** – Aggregate findings from multiple security services *Access Control and Shadow IT Prevention (S 10.16)* **AWS IAM** – Identity and access management	

Summary of requirements	AWS Considerations	Implementation
	AWS Organizations – Service Control Policies (SCPs) to prevent unauthorized service usage **AWS CloudTrail** – Monitor and log all API calls to detect shadow IT **AWS Config** – Detect non-compliant resources and configurations **AWS Control Tower** – Preventive and detective guardrails *Documentation and Audit* **AWS Artifact** – On-demand access to AWS compliance reports and certifications **AWS Systems Manager** – Document and automate operational procedures **AWS CloudFormation** – Infrastructure documentation through code *Third-Party Integration (S 10.12)* **AWS Marketplace** – Vetted third-party software with security assessments **AWS Service Catalog** – Create and manage approved IT service catalogs **AWS Partner Network (APN)** – Access to validated AWS Partners *Additional considerations* - Use the AWS Well-Architected Framework as the foundation for enterprise architecture design. - Implement AWS Organizations with separate accounts for production, development, and testing environments. - Use AWS CodePipeline and related services to automate SDLC processes with integrated security scanning. - Deploy AWS Security Hub and AWS Config for continuous compliance monitoring. - Use Amazon CodeGuru for automated code reviews. - Implement AWS Systems Manager Change Manager for formal change approval processes. - Use AWS CloudTrail and AWS Config to monitor and prevent shadow IT. - Use Amazon Inspector for continuous vulnerability assessment of software dependencies. - Access compliance documentation through AWS Artifact to support audit requirements.	

Patch and End-of-Life System Management

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.17 Financial institutions must ensure systems are free from known security vulnerabilities and not running on outdated/EOL technology by: **(a)** Maintaining current, accurate security baselines for technology component hardening; **(b)** Continuously monitoring and timely implementing latest patches; **(c)** Identifying, planning and implementing remedial actions for systems approaching EOL; and **(d)** Obtaining management approval for exceptions to use unsupported technology, supported by thorough risk assessment, clear phase-out timeline, and annual reviews. **S 10.18** Financial institutions must establish a patch and EOL management framework addressing: **(a)** Identification and risk assessment of technology assets for vulnerabilities from undeployed patches or EOL systems; **(b)** Criteria, priority and turnaround time for patch deployment based on vulnerability severity; **(c)** Compatibility testing before patch deployment to minimize system disruption; **(d)** End-to-end workflow adherence for patch deployment (approval, testing, monitoring, tracking); and **(e)** End-user awareness for orderly transition. **S 10.19** Financial institutions must continually monitor technology effectiveness and security, considering disruptive developments, by: **(a)** Ensuring board receives advice on business impacts from evolving technology;	**Customer responsibility** - Patch Management for Customer-Managed Systems - End-of-Life (EOL) System Management - Vulnerability Management - Board Reporting and Strategy - End-User Awareness *AWS services and resources that can help support this requirement:* *Patch Management Services:* **AWS Systems Manager Patch Manager** – Automates the process of patching managed instances with security-related and other types of updates **AWS Systems Manager** – Provides visibility and control of infrastructure on AWS and helps maintain security baselines *Vulnerability and Compliance Monitoring:* **Amazon Inspector** – Automated security assessment service that helps improve the security and compliance of applications deployed on AWS **AWS Security Hub** – Provides a comprehensive view of security alerts and security posture across AWS accounts **AWS Config** – Continuously monitors and records AWS resource configurations and allows automation of evaluation against desired configurations **AWS Trusted Advisor** – Provides real-time guidance to help provision resources following AWS best practices *Monitoring and Detection:* **Amazon CloudWatch** – Monitors applications, responds to system-wide performance changes, and provides a unified view of operational health **AWS CloudTrail** – Enables governance, compliance, operational auditing, and risk auditing of your AWS account **Amazon GuardDuty** – Threat detection service that continuously monitors for malicious activity and unauthorized behavior *Compliance and Reporting:*	**SEC 1**: How do you securely operate your workload? **SEC 6**: How do you protect your compute resources? **REL 8**: How do you implement change? **COST 10**: How do you evaluate new services? **OPS 10**: How do you manage workload and operations events? **SEC 4**: How do you detect and investigate security events? **OPS 1**: How do you determine what your priorities are? **OPS 5**: How do you reduce defects, ease remediation, and improve flow into production? **REL 12**: How do you test reliability?

Summary of requirements	AWS Considerations	Implementation
(b) Formulating long-term strategy with competent resources to manage risks, including new cyber threats; and **(c)** Establishing system migration roadmap to preserve infrastructure security and reliability.	**AWS Artifact** – Provides on-demand access to AWS security and compliance reports (SOC 1, SOC 2, SOC 3, ISO 27001, and PCI DSS reports) **AWS Audit Manager** – Helps continuously audit AWS usage to simplify risk assessment and compliance *Infrastructure Management:* **AWS Well-Architected Framework** – Helps build secure, high-performing, resilient, and efficient infrastructure with a consistent approach to evaluate architectures *Communication and Awareness:* **AWS Personal Health Dashboard** – Provides a personalized view into the performance and availability of AWS services with relevant and timely information **AWS Security Bulletins** – Keeps customers updated on security announcements	

Cryptography

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.20 Financial institutions must establish a robust cryptography policy addressing: **(a)** Adoption of industry standards for encryption, authentication, signatures, and random number generation **(b)** Secure cryptographic key lifecycle management (generation through destruction) **(c)** Annual review of cryptographic standards for critical and customer-facing systems **(d)** IT asset inventory expansion to include all cryptographic tools with usage rationale and system mapping **(e)** Development and testing of compromise-recovery plans with escalation procedures and containment strategies **S 10.21** Financial institutions must conduct due diligence on cryptographic controls to protect information confidentiality, integrity, authentication, authorization, and non-repudiation, ensuring: **(a)** Retention of encryption key ownership and control (except for non-critical systems without customer data) **(b)** Appropriate measures for secure key management when keys are not self-generated, adhering to industry standards **(c)** Assessment of third-party reliance consistency with risk appetite **(d)** Consideration of system resources and encrypted data visibility risks **S 10.22** Financial institutions must ensure cryptographic controls use suitable protocols based on recognized international standards, with secret and public key protocols providing high protection.	**Shared responsibility** **Customer responsibilities** - Cryptography Policy Development and Implementation - Encryption Key Management and Ownership - Cryptographic Standards Review and Inventory - Compromise Recovery Planning - Certificate Management - Due Diligence and Risk Assessment **AWS responsibilities** *Infrastructure-Level Encryption* - Provide industry-leading encryption features to protect customer content in transit and at rest. - Manage the security of the underlying cloud infrastructure. *Cryptographic Services and Tools* - Offer scalable and efficient encryption capabilities across AWS services. - Provide hardware-based cryptographic key storage options. - Maintain compliance with cryptographic standards and best practices. *Compliance and Assurance* - Maintain certifications and attestations (SOC, ISO, PCI DSS) that validate cryptographic controls. - Provide audit reports through AWS Artifact for customer validation. *AWS services and resources that can help support this requirement:* *Key Management and Encryption Services* **AWS Key Management Service (AWS KMS)** - Centralized key management service for creating and controlling encryption keys. - Supports customer managed keys for full control over encryption keys. - Integrates with most AWS services for seamless encryption. - Provides key lifecycle management, including rotation, deletion, and auditing. - Supports industry-standard cryptographic algorithms. **AWS CloudHSM** - Dedicated hardware security modules (HSMs) for cryptographic key storage.	**SEC 8**: How do you protect your data at rest? **SEC 9**: How do you protect your data in transit? **SEC 2**: How do you manage identities for people and machines? **SEC 3**: How do you manage permissions for people and machines? **SEC 1**: How do you securely operate your workload? **SEC 10**: How do you anticipate, respond to, and recover from incidents? **SEC 6**: How do you protect your compute resources?

Summary of requirements	AWS Considerations	Implementation
Risk-appropriate key storage and encryption/decryption must occur in protected environments (HSM, TEE, or similar devices). **S 10.23** Financial institutions must store public keys in certificates from recognized Certificate Authorities (risk-appropriate). Customer certificates require recognized CAs. Authentication and signature protocols must ensure legally binding, irrefutable private key use. Certificate issuance and renewal must follow industry best practices and legal/regulatory requirements.	- FIPS 140-3 Level 3 validated HSMs for regulatory compliance. - You have exclusive control over keys and cryptographic operations. - Supports both symmetric and asymmetric key operations. - Provides tamper-resistant hardware for private key protection. **AWS Certificate Manager (ACM)** - Manages SSL/TLS certificates from recognized Certificate Authorities. - Automates certificate provisioning, deployment, and renewal. - Integrates with AWS services such as Elastic Load Balancing and CloudFront. - Supports both public and private certificates. **AWS Private Certificate Authority (AWS Private CA)** - Managed private certificate authority service. - Issues and manages private certificates for internal resources. - Supports certificate lifecycle management. *Encryption at Rest Services* **Amazon S3 Encryption** - Server-side encryption with AWS KMS (SSE-KMS) or customer-provided keys (SSE-C). - Client-side encryption options. Bucket-level encryption policies. **Amazon EBS Encryption** - Encryption for Amazon EBS volumes using AWS KMS. - Automatic encryption of data at rest and in transit between instances and volumes. **Amazon RDS Encryption** - Encryption for database instances and snapshots. - Transparent Data Encryption (TDE) support for Oracle and SQL Server. *Encryption in Transit* **AWS VPN and AWS Direct Connect** - Encrypted connections between on-premises and AWS. - IPsec VPN tunnels for secure communication. **TLS/SSL Support** - TLS 1.2 and 1.3 support across AWS services. - Configurable cipher suites for compliance requirements. *Monitoring and Compliance* **AWS CloudTrail** - Logs all API calls, including cryptographic key usage. - Provides audit trail for key management operations. - Supports compliance and forensic investigations.	

Summary of requirements	AWS Considerations	Implementation
	AWS Config - Tracks configuration changes to encryption settings. - Provides compliance checking against cryptographic policies. - Provides inventory of encrypted resources. **AWS Security Hub** - Centralized view of security and compliance status. - Automated compliance checks for encryption standards. - Integration with cryptographic best practices frameworks. *Additional Security Services* **AWS Secrets Manager** - Secure storage and rotation of secrets, API keys, and credentials. - Automatic rotation of secrets with AWS KMS encryption. - Fine-grained access control. **Amazon Macie** - Discovers and protects sensitive data. - Identifies unencrypted data stores. - Provides data classification and protection recommendations. *Additional considerations* - Customer Control: You maintain full control over encryption keys and can choose to manage keys yourself using AWS KMS or AWS CloudHSM. - Industry Standards: AWS cryptographic services support recognized international standards (AES-256, RSA, ECDSA). - Compliance Validation: AWS provides SOC, ISO 27001, PCI DSS, and other compliance reports through AWS Artifact to validate cryptographic controls. - Protected Environments: AWS CloudHSM provides FIPS 140-3 Level 3 validated hardware for storing private keys in protected environments. - Certificate Management: AWS Certificate Manager handles certificates from recognized Certificate Authorities with automated renewal. - Audit and Monitoring: AWS CloudTrail and AWS Config provide logging and monitoring of cryptographic operations for reviews and compromise detection.	

Data Centre Resilience

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.24 Financial institutions must define resilience and availability objectives for data centres aligned with business recovery goals. **S 10.25** Data centres must have redundant capacity components and multiple distribution paths to eliminate single points of failure for business recovery. **S 10.26** Critical systems must be hosted in dedicated, physically secured production data centre space outside disaster-prone areas. Requirements include: - No single point of failure in design and connectivity for critical components (hardware, electrical, thermal, infrastructure) - Adequate maintenance and continuous monitoring with timely fault alerts **S 10.27** Adequate control procedures required for data centre operations, including: - Automated tools for batch processing management - Change management procedures for production systems - Error handling and exceptional condition management **S 10.28** Incompatible activities must be segregated to prevent unauthorised activity. Vendor/programmer access to production environments must be properly authorised and monitored.	**Shared responsibility** **Customer responsibilities** - Defining resilience and availability objectives based on their business recovery requirements and risk assessment processes. - Architecting their workloads to use AWS infrastructure features for redundancy and high availability. - Establishing control procedures - Configuring automated tools for batch processing and operational management. - Implementing proper authorization and monitoring for vendor or programmer access to production environments. - Defining their operational model for managing systems, databases, and services. **AWS Responsibilities** - Physical security of data centers from unauthorized access. - Geographic distribution of infrastructure across multiple Availability Zones and Regions, designed to avoid disaster-prone areas. - Redundant infrastructure components including: a. Electrical power systems with backup power supplies (UPS and onsite generation) b. Multiple independent utility grids feeding each Availability Zone c. Redundant thermal management and climate control systems d. Multiple tier-1 transit provider connections - Eliminating single points of failure in data center design through: a. Independent Availability Zones within each Region b. Separated physical infrastructure c. Redundant network connectivity - Continuous monitoring and preventative maintenance of: a. Electrical and mechanical equipment b. Building management systems c. Environmental controls (temperature and humidity) - High availability infrastructure designed to tolerate system or hardware failures with minimal customer impact. *AWS services and resources that can help support this requirement:* *For Resilience and Availability (S 10.24, S 10.25)*	**REL 13**: How do you plan for disaster recovery (DR)? **REL 10**: How do you use fault isolation to protect your workload? **REL 11**: How do you design your workload to withstand component failures? **REL 6**: How do you monitor workload resources? **REL 8**: How do you implement change? **OPS 10**: How do you manage workload and operations events? **SEC 3**: How do you manage permissions for people and machines? **SUS 1**: How do you select Regions for your workload? **OPS 7**: How do you know that you are ready to support a workload? **OPS 6**: How do you mitigate deployment risks? **SEC 2**: How do you manage identities for people and machines? **SEC 4**: How do you detect and investigate security events?

Summary of requirements	AWS Considerations	Implementation
	AWS Regions and Availability Zones – Deploy across multiple Availability Zones for redundancy and fault tolerance. **Amazon Elastic Compute Cloud (Amazon EC2)** – Instance placement across multiple Availability Zones. **Amazon Relational Database Service (Amazon RDS)** – Multi-AZ deployments for database redundancy. **Elastic Load Balancing** – Distribute traffic across multiple Availability Zones. **Amazon Simple Storage Service (Amazon S3)** – Automatic data replication across multiple facilities. *For Monitoring and Control (S 10.26, S 10.27)* **Amazon CloudWatch** – Monitor applications, set alarms, and track metrics for operational health. **AWS CloudTrail** – Monitor and record account activity for audit and compliance. **AWS Config** – Assess, audit, and evaluate configurations of AWS resources. **AWS Systems Manager** – Automate operational tasks and manage batch processing. **AWS Personal Health Dashboard** – Personalized view of service availability and scheduled events. *For Access Control and Segregation (S 10.28)* **AWS Identity and Access Management (IAM)** – Control user and programmatic access with granular policies. **AWS Organizations** – Manage multiple accounts with centralized governance. **Multi-factor authentication (MFA)** – Require strong authentication for sensitive access. **IAM roles** – Provide secure, temporary access for vendors or programmers. AWS CloudTrail – Log and monitor all access activities for audit purposes. *For Change Management and Error Handling (S 10.27)* **AWS Systems Manager Change Manager** – Automate change request workflows. **AWS Lambda** – Automate error handling and exception management. **Amazon EventBridge** – Route operational events for automated responses. **AWS Step Functions** – Orchestrate batch processes and workflows. *Key Infrastructure Features* **Data Center Design:** - Each Availability Zone is designed as an independent failure zone. - Physical separation within metropolitan regions. - Located in lower-risk flood plains.	

Summary of requirements	AWS Considerations	Implementation
	- Discrete UPS and onsite backup generation per Availability Zone. - Fed by different grids from independent utilities. - Redundantly connected to multiple tier-1 transit providers. **Compliance and Assurance:** - ISO 27001 certified Information Security Management System. - ISO 22301:2019 Business Continuity Management System certification. - SOC 1, SOC 2, and SOC 3 reports available through AWS Artifact. - Regular third-party audits and assessments. You can validate AWS infrastructure controls through compliance reports available in AWS Artifact.	

Service Availability

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.29 Financial institutions must plan and manage system capacity considering peak periods, business growth, and technology changes. **S 10.30** Financial institutions must establish real-time monitoring for capacity utilization and performance of key processes/services, with actionable alerts for administrators. Monitoring scope, metrics, and thresholds require periodic updates. **S 10.31** Financial institutions shall enhance resilience of key digital services and delivery channels through: **(a)** Implement mechanisms by 30 Sept 2027 to: **(i)** Detect failed transactions and measure service availability accurately; **(ii)** Monitor affected customers and transaction volumes during disruptions; **(iii)** Escalate to senior management when disruptions affect ≥5% of expected daily customers/volumes; **(b)** Conduct regular reviews to identify and mitigate vulnerable IT interdependencies; **(c)** Establish stand-in processing arrangements by 30 Sept 2027, prioritizing least substitutable services, with clear customer communication on terms, risks, and fraud mitigation. **S 10.32** Critical systems must be designed for high availability with: - Maximum 4 hours cumulative unplanned downtime per rolling 12 months - Maximum 120 minutes tolerable downtime per incident **G 10.33** Eligible e-money issuers, non-bank merchant acquirers, and intermediary remittance	**Shared responsibility** **Customer responsibilities** - Capacity Planning and Management (S 10.29) - Real-time Monitoring (S 10.30) - Resilience Enhancement (S 10.31) - High Availability Design (S 10.32) - Technology Diversity (S 10.34) - Incident Response (S 10.35) - Quarterly Reporting (S 10.35(e) **AWS Responsibilities** *Infrastructure Availability* - Maintain high availability of AWS global infrastructure designed to tolerate system or hardware failures with minimal customer impact. - Design data centers to anticipate and tolerate failure while maintaining service levels. - Provide multiple Availability Zones within each AWS Region, designed as independent failure zones. - Make sure Availability Zones are physically separated, located in lower risk flood plains, and fed by different power grids from independent utilities. - Maintain redundant connections to multiple tier-1 transit providers. *Monitoring and Alerting Services* - Provide monitoring services and tools for customers to track performance and availability. - Offer the AWS Health Dashboard for personalized views of service performance and availability. - Deliver relevant and timely information through AWS Health events. - Provide proactive notifications to help customers plan for scheduled activities. *Service Level Agreements* - Offer Service Level Agreements (SLAs) for paid, generally available services.	**OPS 8**: How do you utilize workload observability in your organization? **OPS 9**: How do you understand the health of your operations? **OPS 10**: How do you manage workload and operations events? **REL 6**: How do you monitor workload resources? **REL 7**: How do you design your workload to adapt to changes in demand? **REL 10**: How do you use fault isolation to protect your workload? **REL 11**: How do you design your workload to withstand component failures? **REL 12**: How do you test reliability? **REL 13**: How do you plan for disaster recovery (DR)? **COST 9**: How do you manage demand, and supply resources? **OPS 2**: How do you structure your organization to support your business outcomes? **OPS 4**: How do you implement observability in your workload?

Summary of requirements	AWS Considerations	Implementation
institutions (non-NCII) are encouraged to implement paragraph 10.31 measures. **S 10.34** Financial institutions shall prioritize technology diversity to prevent excessive exposure to similar technology risks in critical systems. **S 10.35** During service interruptions, financial institutions shall: **(a)** Ensure timely escalation and resume services within paragraph 10.32 timeframes; **(b)** Define clear accountabilities and formalize third-party arrangements for coordination; **(c)** Establish communication plans to inform customers, manage feedback, provide updates, and offer alternatives; **(d)** Provide convenient means for customers to check service availability (e.g., real-time status on website); **(e)** Disclose quarterly service availability track record within 15 days of quarter-end, starting 15 Oct 2027.	- Make SLAs publicly available at https://aws.amazon.com/legal/service-level-agreements. *Business Continuity* - Maintain and test the AWS Business Continuity Plan. - Implement ISO 22301:2019 certified Business Continuity Management System (BCMS). *Compliance and Assurance* - Provide independent third-party audit reports and certifications (SOC 1, SOC 2, SOC 3, ISO 27001, ISO 27017, ISO 27018, ISO 22301, PCI DSS). - Make compliance reports available through AWS Artifact. *AWS services and resources that can help support this requirement:* *Capacity Planning and Scaling* **AWS Auto Scaling** – Automatically adjust capacity to maintain steady, predictable performance at the lowest possible cost. **AWS Compute Optimizer** – Recommends optimal AWS resources for workloads to reduce costs and improve performance. **AWS Trusted Advisor** – Provides recommendations for cost optimization, performance, security, and fault tolerance. *Monitoring and Alerting (S 10.30)* **Amazon CloudWatch** – Monitor applications, respond to system-wide performance changes, optimize resource use, and get unified view of operational health. - Set custom performance metrics and thresholds. - Configure alarms for unusual activity. - Collect and track metrics, collect and monitor log files. **AWS CloudTrail** – Monitor and record account activity across AWS infrastructure, capture comprehensive history of changes. **AWS Health Dashboard** – Personalized view of AWS service performance and availability with proactive notifications. **AWS Personal Health Dashboard** – Displays relevant and timely information for managing events in progress. *High Availability and Resilience (S 10.31, S 10.32)* **Multiple AWS Regions** – Deploy across multiple geographic Regions for greater separation and disaster recovery. **Multiple Availability Zones** – Deploy across multiple Availability Zones within a Region for independent failure zones.	**REL 3**: How do you design your workload service architecture? **SEC 10**: How do you anticipate, respond to, and recover from incidents?

Summary of requirements	AWS Considerations	Implementation
	- Each Availability Zone designed with independent power, cooling, and networking. - Physically separated within metropolitan Regions. - Connected with high-bandwidth, low-latency networking. **Amazon Route 53** – Highly available and scalable DNS web service with health checks and failover capabilities. **Elastic Load Balancing** – Automatically distribute incoming application traffic across multiple targets. **AWS Elastic Disaster Recovery** – Minimize downtime and data loss with fast, reliable recovery. *Service Availability Monitoring* **Amazon CloudWatch Synthetics** – Create canaries to monitor endpoints and APIs, simulate customer interactions. **AWS X-Ray** – Analyze and debug distributed applications to identify performance bottlenecks. **Amazon CloudWatch ServiceLens** – Visualize and analyze health, performance, and availability of applications. *Incident Detection and Response (S 10.35)* **Amazon GuardDuty** – Continuously monitor for malicious activity and unauthorized behavior. **AWS Security Hub** – Centralized view of security alerts and compliance status. **AWS Config** – Assess, audit, and evaluate configurations of AWS resources. **Amazon EventBridge** – Build event-driven architectures for automated responses to operational changes. **AWS Systems Manager Incident Manager** – Automate response plans and collaborate during incidents. *Technology Diversity (S 10.34)* **Multiple AWS Regions and Availability Zones** – Geographic and infrastructure diversity. **Diverse compute options** – Amazon EC2, AWS Lambda, Amazon ECS, Amazon EKS, AWS Fargate for different architectural approaches. **Multiple database engines** – Amazon RDS (multiple engines), Amazon DynamoDB, Amazon DocumentDB, Amazon Neptune for database diversity. **Hybrid architectures** – AWS Outposts, AWS Direct Connect for on-premises integration. *Communication and Status Updates (S 10.35)*	

Summary of requirements	AWS Considerations	Implementation
	Amazon Simple Notification Service – Send notifications to customers through multiple channels. **Amazon Simple Email Service** – Send bulk email communications to customers. **AWS Service Health Dashboard** – Public view of AWS service status. **Amazon CloudWatch Dashboards** – Create customized views of metrics and alarms for real-time status. *Backup and Recovery* **AWS Backup** – Centralized backup service to automate and manage backups. **Amazon S3** – Durable object storage for backup data with multiple storage classes. **Amazon EBS Snapshots** – Point-in-time backups of Amazon EBS volumes. **Amazon RDS Automated Backups** – Automated backups with point-in-time recovery. *Performance Optimization* **AWS Well-Architected Framework** – Best practices for building secure, high-performing, resilient, and efficient infrastructure. - Operational Excellence pillar - Performance Efficiency pillar - Reliability pillar **AWS Resilience Hub** – Prepare and protect applications from disruptions.	

Network Resilience

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.36 Financial institutions must design and implement reliable, scalable, and secure enterprise networks supporting business activities and future growth. **S 10.37** Network services for critical systems must be reliable with no single point of failure to protect against network faults and cyber threats. **G 10.38** Control measures should include component redundancy, service diversity, and alternate network paths. **S 10.39** Financial institutions must establish real-time bandwidth monitoring processes and resilience metrics to detect over-utilization, disruptions, congestion, and faults, including traffic analysis for trends and anomalies. **S 10.40** Network services supporting critical systems must ensure data confidentiality, integrity, and availability. **S 10.41** Financial institutions must maintain a network design blueprint identifying all internal and external interfaces, connectivity, and segmentations (both physical and logical). **S 10.42** Network device logs must be retained for at least three years for investigations and forensic purposes. **S 10.43** Financial institutions must implement safeguards (such as logical network segmentation) to	**Shared responsibility** **Customer responsibilities** - Network Architecture Design - Network Segmentation - Monitoring and Metrics - Data protection - Logging and Retention - Access Control **AWS Responsibilities** *Infrastructure Resilience:* - Design and maintain highly available network infrastructure - Operate multiple Availability Zones within each AWS Region - Make sure that Availability Zones are physically separated and independently operated - Provide redundant connectivity between Availability Zones through multiple tier-1 transit providers *Physical Network Security:* - Secure the physical network infrastructure - Maintain redundant power supplies and network connectivity - Protect against environmental risks at data center locations *Network Performance:* - Monitor and maintain AWS global network infrastructure - Provide network capacity and performance standards *AWS services and resources that can help support this requirement:* *Network Design and Redundancy (S 10.36, S 10.37, G 10.38)* **Amazon Virtual Private Cloud (Amazon VPC)**: Create isolated network environments with custom IP ranges, subnets, and routing tables. **AWS Transit Gateway**: Connect multiple VPCs and on-premises networks through a central hub. **Elastic Load Balancing**: Distribute traffic across multiple targets in multiple Availability Zones for high availability.	**SEC 5**: How do you protect your network resources? **REL 2**: How do you plan your network topology? **REL 10**: How do you use fault isolation to protect your workload? **REL 11**: How do you design your workload to withstand component failures? **REL 6**: How do you monitor workload resources? **PERF 4**: How do you select and configure networking resources in your workload? **SEC 4**: How do you detect and investigate security events? Supporting Best Practices **REL 4**: How do you design interactions in a distributed system to prevent failures? **REL 5**: How do you design interactions in a distributed system to mitigate or withstand failures? **SEC 9**: How do you protect your data in transit? **OPS 10**: How do you manage workload and operations events? **REL 12**: How do you test reliability?

Summary of requirements	AWS Considerations	Implementation
minimize risk of system compromise spreading between group entities.	**AWS Direct Connect**: Establish dedicated network connections with redundant connections for reliability. **Amazon Route 53**: DNS service with health checks and failover routing policies. **Multiple Availability Zones**: Deploy resources across multiple Availability Zones within a Region for component redundancy. *Network Monitoring and Bandwidth Management (S 10.39)* **Amazon CloudWatch**: Monitor network metrics, set alarms for bandwidth utilization, and track performance. **VPC Flow Logs**: Capture information about IP traffic going to and from network interfaces. **AWS Network Manager**: Monitor and manage global networks with visibility into network performance. **Amazon CloudWatch Network Monitor**: Monitor network performance between AWS and on-premises environments. **AWS Transit Gateway Network Manager**: Visualize and monitor global network topology. *Data Confidentiality, Integrity, and Availability (S 10.40)* **AWS Certificate Manager (ACM)**: Provision and manage SSL/TLS certificates for encryption in transit. **AWS Key Management Service (AWS KMS)**: Manage encryption keys for data protection. **VPC security groups**: Control inbound and outbound traffic at the instance level. Network access control lists (network ACLs): Provide stateless filtering at the subnet level. **AWS PrivateLink**: Access services privately without exposing traffic to the public internet. **AWS Shield**: DDoS protection (Standard and Advanced tiers). **AWS WAF**: Web application firewall to protect against common web exploits. *Network Documentation and Blueprint (S 10.41)* **AWS Config**: Track and record AWS resource configurations and relationships. **AWS Systems Manager**: Document and visualize network architecture. **AWS Resource Groups**: Organize and manage AWS resources. **VPC Reachability Analyzer**: Analyze and debug network reachability between resources. *Network Logging and Retention (S 10.42)* **VPC Flow Logs**: Capture network traffic logs with configurable retention periods.	

Summary of requirements	AWS Considerations	Implementation
	AWS CloudTrail: Log API calls and network-related events with long-term retention. **Amazon CloudWatch Logs**: Centralize and retain logs with customizable retention (three years or more). **Amazon S3**: Store logs with lifecycle policies for long-term archival. **AWS CloudTrail Lake**: Query and analyze CloudTrail events for up to seven years. *Network Segmentation and Isolation (S 10.43)* **Amazon VPC**: Create isolated virtual networks with separate IP address ranges. **VPC peering**: Connect VPCs with controlled routing. **AWS Transit Gateway**: Implement hub-and-spoke network topology with route isolation. **Security groups and network ACLs**: Implement granular network access controls. **AWS Organizations**: Manage multiple AWS accounts with Service Control Policies (SCPs). **AWS Resource Access Manager**: Share resources across accounts while maintaining isolation. **AWS PrivateLink**: Turn on private connectivity between VPCs without network overlap. *Additional Considerations* **Multi-Region Architecture**: For enhanced resilience, you can deploy across multiple AWS Regions. **Compliance Validation**: AWS provides compliance reports through AWS Artifact (SOC 2, ISO 27001, and others) that you can use to validate network security controls. **Well-Architected Framework**: Reference the AWS Well-Architected Framework, particularly the Reliability and Security pillars, for network design best practices.	

System backup and restoration

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.44 Financial institutions must establish robust backup strategy and procedures: **(a)** Establish backup and restoration procedures for data lifecycle management **(b)** Maintain adequate backup copies of critical data, OS software, production programs, system utilities, master/transaction files, and event logs **(c)** Store backup media in environmentally secure, access-controlled sites **(d)** Secure storage and transportation of sensitive data on removable media per Appendix 1 standards **(e)** Periodically test backup/restoration procedures; promptly remediate failed backups **(f)** Conduct independent risk assessment of end-to-end backup storage and delivery management for adequate data protection **S 10.45** Financial institutions shall establish tamper-proof backup arrangements and isolated recovery environments to enable timely resumption of critical services during destructive cyber-attacks (e.g., ransomware).	**Customer responsibility** - Defining and implementing backup strategies that meet your business recovery objectives and regulatory requirements - Establishing backup and restoration procedures to manage the backup data lifecycle - Configuring backup policies - Testing backup and restoration procedures periodically to validate recovery capabilities - Taking remedial actions promptly to fix root causes of unsuccessful backups Implementing access controls for backup data and storage locations - Encrypting backup data both at rest and in transit to protect sensitive information - Establishing tamper-proof backup arrangements and isolated recovery environments for critical systems - Conducting independent risk assessments of end-to-end backup storage and delivery management - Maintaining backup copies *AWS services and resources that can help support this requirement:* **AWS Backup** A centralized backup service to automate and manage backups across AWS services. AWS Backup supports backup policies, retention management, and lifecycle policies. The service provides backup vault lock for tamper-proof, immutable backups and can create cross-Region and cross-account backup copies. **Amazon S3 (Amazon Simple Storage Service)** Amazon S3 provides highly durable storage (99.999999999% durability) for backup data. Amazon S3 features include: - S3 Versioning to maintain multiple versions of objects - S3 Object Lock for immutable storage (WORM - Write Once Read Many) - S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, and S3 Glacier Deep Archive for long-term, cost-effective backup storage - Cross-Region Replication (CRR) for geographic redundancy **Amazon EBS Snapshots** Amazon Elastic Block Store (Amazon EBS) provides point-in-time snapshots of EBS volumes. Snapshots are incremental backups stored in Amazon S3 and can be copied across Regions for disaster recovery. **AWS Storage Gateway**	**REL 9**: How do you back up data? **REL 13**: How do you plan for disaster recovery (DR)? **REL 12**: How do you test reliability? **SEC 8**: How do you protect your data at rest? **REL 10**: How do you use fault isolation to protect your workload? **SEC 10**: How do you anticipate, respond to, and recover from incidents? **SEC 9**: How do you protect your data in transit?

Summary of requirements	AWS Considerations	Implementation
	A hybrid cloud storage service for on-premises backup to AWS. AWS Storage Gateway supports tape gateway for virtual tape library backups.	

Third Party Service Provider Management

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.46 Board and senior management must exercise effective oversight when engaging third party service providers for critical technology functions. Financial institutions remain accountable for managing all associated risks and ensuring compliance with regulatory requirements. **S 10.47** Financial institutions must conduct due diligence on third party service providers before on-boarding and throughout engagement to ensure business performance and recovery objectives are met, considering current risk environment and risks outlined in Appendix 8. **S 10.48** Financial institutions must establish Service Level Agreements (SLA) containing minimum requirements: **(a)** Regulator access rights to records, files, data, and management information **(b)** Prior notice requirements for substantial sub-contracting **(c)** Written undertaking on secrecy provisions and confidentiality (continuing post-engagement) **(d)** Disaster recovery and backup arrangements **(e)** Service level objectives for uptime/availability **(f)** Business continuity arrangements for exit/termination, including timely data recovery **(g)** Prompt disclosure of service disruptions or cyber incidents affecting the institution or customer data **(h)** Compliance with international standards and staff certification requirements **(i)** Participation in security awareness and education programs	**Customer responsibility** - Governance and Oversight - Due Diligence and Vendor Assessment - Service Level Agreements - Continuous Monitoring *AWS services and resources that can help support this requirement:* *Monitoring and Continuous Assessment* **AWS CloudTrail** – Monitor and record account activity across AWS infrastructure. Amazon CloudWatch – Centralize logs, monitor applications, and set alarms for operational health. **AWS Config** – Continually assess, audit, and evaluate configurations and relationships of resources. **Amazon GuardDuty** – Continuously monitor for malicious activity and unauthorized behavior. **AWS Security Hub** – Centralized view of security alerts and compliance status. **AWS Health Dashboard** – Real-time information on service availability and personalized event notifications. *Audit and Compliance* **AWS Artifact** – On-demand access to security and compliance reports (SOC 1/2/3, ISO certifications, PCI DSS reports). **AWS Audit Manager** – Facilitate audits and continuous compliance assessment. **AWS Trusted Advisor** – Best practice recommendations for security, performance, and cost optimization. *Security and Access Control* **AWS Identity and Access Management (IAM)** – Control user and programmatic access with granular policies. **AWS Organizations** – Centrally manage and govern multiple AWS accounts. **AWS Key Management Service (AWS KMS)** – Manage encryption keys. **AWS CloudHSM** – Hardware-based cryptographic key storage. *Business Continuity and Disaster Recovery* **AWS Resilience Hub** – Assess and improve application resilience.	**OPS 2**: How do you structure your organization to support your business outcomes? **OPS 7**: How do you know that you are ready to support a workload? **OPS 9**: How do you understand the health of your operations? **OPS 10**: How do you manage workload and operations events? **SEC 1**: How do you securely operate your workload? **SEC 10**: How do you anticipate, respond to, and recover from incidents? **REL 11**: How do you design your workload to withstand component failures? **REL 13**: How do you plan for disaster recovery (DR)? **OPS 1**: How do you determine what your priorities are? **SEC 2**: How do you manage identities for people and machines? **SEC 3**: How do you manage permissions for people and machines? **SEC 4**: How do you detect and investigate security events?

Summary of requirements	AWS Considerations	Implementation
S 10.49 Financial institutions must formulate a roadmap for continuous monitoring of third party cybersecurity posture, including: **(a)** Measure IT infrastructure footprint and customer information accessible to third parties; manage external exposures **(b)** Adopt security policies to mitigate third party risks **(c)** Ensure incident response plans include third party protocols for security vulnerabilities **(d)** Define priority security controls requiring frequent assurance **(e)** Monitor technology and cyber incidents at higher frequency **(f)** Implement automated metric testing solutions **(g)** Establish processes for responding to breached thresholds and remedying control gaps	**Multiple AWS Regions and Availability Zones** – Geographic redundancy and fault isolation. **AWS Backup** – Centralized backup management. *Incident Response* **AWS Security Bulletins** – Stay updated on security announcements. *Additional considerations* - Use AWS Artifact to access compliance reports and validate AWS controls against regulatory requirements. - Implement the AWS Well-Architected Framework to build secure, high-performing, resilient infrastructure. - Use AWS monitoring services (CloudTrail, CloudWatch, Config, GuardDuty, Security Hub) to achieve continuous monitoring of cybersecurity posture. - Review AWS compliance certifications regularly to make sure they align with internationally recognized standards (ISO 27001, SOC 2, PCI DSS). - Establish clear delineation of responsibilities between you and AWS as outlined in the Shared Responsibility Model and formalized in the Enterprise Agreement.	**SEC 5**: How do you protect your network resources? **SEC 6**: How do you protect your compute resources? **REL 6**: How do you monitor workload resources? **REL 10**: How do you use fault isolation to protect your workload? **REL 12**: How do you test reliability?

Cloud Services

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.50 Financial institutions must conduct comprehensive risk assessment before cloud adoption, addressing: **(a)** Deployment model sophistication **(b)** System migration to cloud **(c)** Infrastructure location, geo-political and legal risks **(d)** Multi-tenancy/data co-mingling **(e)** Vendor lock-in and portability **(f)** Security configuration customization capability **(g)** Cyber-attack exposure via providers **(h)** Service termination and data security **(i)** Responsibility and liability demarcation **(j)** Ongoing regulatory compliance ability **G 10.51** For critical systems on public cloud, institutions should follow Appendix 10 risk controls or demonstrate alternative practices are equally/more effective to the Bank. **S 10.52** Financial institutions must implement safeguards for customer, counterparty, and proprietary data on cloud services, maintaining ownership, control, and management of all data and cryptographic keys.	**Shared responsibility** **Customer responsibilities** - Risk Assessment and Cloud Adoption - Data Control and Ownership - Security configuration **AWS Responsibilities** *Infrastructure Security* - AWS manages security of the cloud and makes sure that AWS infrastructure complies with global regulatory requirements and best practices. - AWS provides the underlying infrastructure with high availability and resilience features. - AWS maintains physical security of data centers and facilities. - AWS implements controls to prevent cross-tenant access and data co-mingling. *Compliance and Assurance* - AWS provides independent third-party audit reports and certifications that are available through AWS Artifact. - AWS maintains compliance with international standards (ISO 27001, 27017, 27018, SOC 1/2/3, PCI DSS). - AWS undergoes regular external audits by independent auditors. *Data Sovereignty* - AWS doesn't move or replicate your content outside your chosen AWS Regions without your agreement. - AWS provides mechanisms to restrict operations to specific geographic Regions. *AWS services and resources that can help support this requirement:* *Risk Assessment and Monitoring* **AWS Audit Manager** – Facilitates continuous auditing and compliance assessments. **AWS Security Hub** – Provides comprehensive security posture management. **AWS Config** – Tracks resource configurations and compliance. **AWS Trusted Advisor** – Offers best practice recommendations. **AWS Well-Architected Framework** – Provides a structured approach to evaluate architectures across six pillars.	**SEC 1**: How do you securely operate your workload? **SEC 2**: How do you manage identities for people and machines? **SEC 3**: How do you manage permissions for people and machines? **SEC 7**: How do you classify your data? **SEC 8**: How do you protect your data at rest? **SEC 9**: How do you protect your data in transit? **SUS 1**: How do you select Regions for your workload? **SEC 5**: How do you protect your network resources? **SEC 6**: How do you protect your compute resources? **SEC 10**: How do you anticipate, respond to, and recover from incidents? **REL 3**: How do you design your workload service architecture? **REL 10**: How do you use fault isolation to protect your workload? **REL 13**: How do you plan for disaster recovery (DR)? **PERF 1**: How do you select appropriate cloud resources and architecture patterns for your workload?

Summary of requirements	AWS Considerations	Implementation
	Data Protection and Encryption **AWS Key Management Service (AWS KMS)** – Centralized key management with customer control. **AWS CloudHSM** – Hardware-based key storage for regulatory compliance. **Amazon S3 encryption** – Server-side and client-side encryption options. **Amazon EBS encryption** – Encryption for block storage volumes. *Access Control and Identity Management* **AWS Identity and Access Management (IAM)** – Granular access control and permission management. **AWS Organizations** – Centralized governance across multiple accounts. **AWS IAM Access Analyzer** – Identifies unintended access to resources. *Monitoring and Logging* **AWS CloudTrail** – Comprehensive audit logging of account activity. **Amazon CloudWatch** – Monitoring and alerting for resources and applications. **Amazon GuardDuty** – Threat detection and continuous security monitoring. **AWS Security Hub** – Centralized security findings aggregation. *Multi-Region and Availability* **AWS Regions and Availability Zones** – Geographic distribution for resilience. **AWS Account Management** – Region restriction capabilities. **Cross-Region Replication** – Data redundancy across geographic locations. *Compliance and Reporting* **AWS Artifact** – On-demand access to compliance reports and certifications. **AWS Compliance Programs** – Documents adherence to regulatory frameworks. *Data Portability and Exit Strategy* **AWS Database Migration Service** – Facilitates data migration in and out of AWS. **AWS Snowball** – Physical data transfer for large datasets. **AWS DataSync** – Automated data transfer service.	

Access Control

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 10.53 Financial institutions must implement access control policies for identification, authentication, and authorization of all users to IT assets and data, with granularity matching the risk level. **S 10.54** Financial institutions shall adhere to these principles: **(a)** "Deny all" default policy - all access must be explicitly authorized **(b)** "Least privilege" - minimum necessary permissions on "need-to-have" basis **(c)** Time-bound access - restricted to specific periods based on work nature **(d)** Segregation of incompatible functions - no single person controls entire operations, including: (i) System development and technology operations (ii) Security administration and system administration (iii) Network operation and network security (iv) IT operations environment **(e)** Establish dual authorization criteria for specific activities **(f)** Robust authentication based on IT asset criticality: (i) Stronger authentication for critical/high-risk activities (e.g., remote access) (ii) Robust identity verification to prevent impersonation (iii) Unique credentials per user for accountability **S 10.55** Must employ multi-factor authentication (MFA) combining 2+ factors (knowledge, inherent/biometric, possession) for critical system access, defending against social engineering.	**Customer responsibility** Customers are responsible for implementing and managing access control policies for their AWS environments, including the principles defined in S 10.54 *AWS services and resources that can help support this requirement:* *Identity and Access Management* **AWS Identity and Access Management (IAM)**: Control user and programmatic access to AWS services and resources with granular policies. Supports: - Deny-all-by-default policies - Least privilege access through fine-grained permissions - Time-bound access through temporary credentials - Segregation of duties through separate policies and roles - Unique user identities for accountability **AWS Organizations**: Manage access controls across multiple AWS accounts, including: - Service Control Policies (SCPs) for centralized access control - Account-level access restrictions *Multi-Factor Authentication* **AWS IAM MFA**: Supports multi-factor authentication that combines knowledge factors (passwords) with possession factors (hardware or virtual MFA devices, security keys) **AWS IAM Identity Center (successor to AWS Single Sign-On)**: Centralized MFA enforcement across AWS accounts *Authentication and Authorization* **AWS IAM Roles**: Turn on temporary, time-bound access with automatic credential rotation **AWS IAM Identity Center**: Centralized identity management with support for external identity providers **AWS IAM Access Analyzer**: Helps identify resources shared with external entities and validate least privilege access *Monitoring and Logging*	**SEC 2**: How do you manage identities for people and machines? **SEC 3**: How do you manage permissions for people and machines? **SEC 4**: How do you detect and investigate security events? **SEC 1**: How do you securely operate your workload? **SEC 10**: How do you anticipate, respond to, and recover from incidents?

Summary of requirements	AWS Considerations	Implementation
S 10.56 Must establish and periodically review a user access matrix outlining access rights, roles/profiles, and authorization authorities. **S 10.57** Must ensure: **(a)** Effective management and monitoring of enterprise-wide system access controls **(b)** Prompt investigation of anomalies to contain cyber incidents **(c)** Activity logging in critical systems for audit/investigations, maintained for 3+ years with timely regular reviews	**AWS CloudTrail**: Records account activity and API calls across AWS infrastructure, providing: - Comprehensive audit trails of user activities - Log retention capabilities (can be configured for 3+ years) - Integration with CloudWatch for real-time monitoring **Amazon CloudWatch**: Monitors applications and resources, providing: - Real-time log analysis - Anomaly detection through CloudWatch Alarms - Centralized log aggregation from multiple sources **AWS Config**: Continuously assesses, audits, and evaluates configurations and relationships of resources **Amazon GuardDuty**: Continuously monitors for malicious activity and unauthorized behavior **AWS Security Hub**: Provides centralized security and compliance monitoring across AWS accounts *Access Control Management* **AWS IAM Access Analyzer**: Analyzes resource policies to help maintain least privilege access **AWS Secrets Manager**: Securely stores and rotates credentials **AWS Systems Manager Session Manager**: Provides secure, auditable access to instances without requiring open inbound ports *Audit and Compliance* **AWS Artifact**: Provides on-demand access to AWS security and compliance reports (SOC 1, SOC 2, SOC 3, ISO 27001, PCI DSS, and others)	

Cyber Risk Management

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 11.1 Financial institutions must ensure enterprise-wide focus on cyber risk management as a collective responsibility across business and technology lines. **S 11.2** Financial institutions must develop a Cyber Risk Framework (CRF) that: Articulates governance for managing cyber risks Defines cyber resilience objectives and risk tolerance Considers evolving cyber threats Ensures operational resilience against extreme but plausible cyber-attacks Supports IPDRR (Identification, Protection, Detection, Response, Recovery) for on-premises and third-party hosted systems **S 11.3** The CRF must include minimum elements: **(a)** Understanding of cyber risk context relative to business operations and cybersecurity posture **(b)** Identification, classification, and prioritization of critical systems, information, assets, and interconnectivity **(c)** Identification of threats, vulnerabilities, and countermeasures for digital services **(d)** Enhanced cyber defense layers using international standards (zero-trust, defense-in-depth, security by design) **(e)** Timely incident detection through continuous monitoring **(f)** Incident handling policies and crisis response playbook for swift recovery **(g)** Policies for secure information sharing with other financial institutions **(h)** Centralized automated system for technology asset inventory tracking	**Customer responsibility** - Cyber Risk Framework (CRF) Development & Governance - Asset Identification & Classification - Threat & Vulnerability Management - Security Controls Implementation - Detection & Monitoring - Incident Response & Recovery - Information Sharing & Collaboration *AWS services and resources that can help support this requirement:* *Asset Management & Inventory (S 11.3h)* **AWS Config** - Continuously assess, audit, and evaluate configurations and relationships of resources. **AWS Systems Manager Inventory** - Collect metadata from managed instances for centralized asset tracking. *Threat & Vulnerability Detection (S 11.3c, e)* **Amazon GuardDuty** - Continuous security monitoring for malicious activity and unauthorized behavior. **AWS Security Hub** - Centralized view of security alerts and compliance status across AWS accounts. **Amazon Inspector** - Automated vulnerability management service for workloads. **AWS Security Bulletins** - Stay updated on security announcements. *Identity & Access Management (S 11.3d - Zero Trust)* **AWS Identity and Access Management (IAM)** - Control user and programmatic access with granular policies. **AWS Organizations** - Centrally manage and govern multiple AWS accounts. **AWS IAM Identity Center** - Manage workforce access to accounts and applications. *Network Security & Defense-in-Depth (S 11.3d)* **AWS WAF (Web Application Firewall)** - Protect web applications from common exploits. **AWS Shield** - Managed DDoS protection (Standard and Advanced tiers). **AWS Network Firewall** - Deploy network security across VPCs.	**SEC 1**: How do you securely operate your workload? **SEC 2**: How do you manage identities for people and machines? **SEC 3**: How do you manage permissions for people and machines? **SEC 4**: How do you detect and investigate security events? **SEC 5**: How do you protect your network resources? **SEC 6**: How do you protect your compute resources? **SEC 7**: How do you classify your data? **SEC 8**: How do you protect your data at rest? **SEC 9**: How do you protect your data in transit? **SEC 10**: How do you anticipate, respond to, and recover from incidents? **OPS 4**: How do you implement observability in your workload? **OPS 10**: How do you manage workload and operations events? **REL 12**: How do you test reliability?

Summary of requirements	AWS Considerations	Implementation
(i) Cyber risk management function (in-house or parent/group) for threat analysis and escalation **NCII Compliance**: Institutions designated as National Critical Information Infrastructure must comply with Cyber Security Act 2024 requirements and NACSA directives. **Control Measures**: Financial institutions must adopt robust controls per Appendix 5 to enhance cyber resilience. **Red Team Testing**: Conduct realistic "Red Team" simulation attacks at least once every three years. **G 11.7** Financial institutions may implement crowdsourced security testing programs via reputable service providers as complement to existing assessments.	**Amazon VPC** - Isolated cloud resources with security groups and network ACLs. **AWS PrivateLink** - Private connectivity between VPCs and services. *Data Protection & Encryption (S 11.3d)* **AWS Key Management Service (AWS KMS)** - Create and control encryption keys. **AWS CloudHSM** - Hardware-based key storage with FIPS-validated HSMs - FIPS 140-3 Security Level 3 **AWS Certificate Manager** - Provision and manage SSL/TLS certificates. **Amazon Macie** - Discover and protect sensitive data by using machine learning. *Monitoring & Detection (S 11.3e)* **Amazon CloudWatch** - Monitor applications, performance changes, centralize logs. **AWS CloudTrail** - Track user activity and API usage across AWS infrastructure. **Amazon Detective** - Analyze and investigate potential security issues. **AWS Config Rules** - Evaluate resource configurations against desired settings. *Incident Response & Recovery (S 11.3f)* **AWS Backup** - Centralized backup service across AWS services. **AWS Resilience Hub** - Assess and improve application resilience. **AWS Systems Manager Incident Manager** - Respond to and resolve incidents. **Amazon EventBridge** - Event-driven automation for incident response. *Compliance & Audit (S 11.2, 11.4)* **AWS Artifact** - On-demand access to AWS compliance reports (SOC, PCI, ISO). **AWS Audit Manager** - Continuously audit AWS usage to simplify risk assessment. **AWS Trusted Advisor** - Real-time guidance to provision resources following AWS best practices. *Security Assessment (S 11.6, G 11.7)* **AWS Penetration Testing** - Conduct security assessments against your AWS infrastructure (some services pre-approved). **AWS Security Hub** - Automated security checks *Threat Intelligence & Information Sharing (S 11.3g)* **AWS Personal Health Dashboard** - Personalized view of service performance and availability with proactive notifications. **AWS Security Hub** - Aggregate and prioritize security findings from multiple AWS services and third-party tools.	

Cybersecurity Operations

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 11.8 - Financial institutions must establish clear cybersecurity responsibilities and implement mitigating measures across all seven phases of the cyber-attack lifecycle: (a) reconnaissance; (b) weaponisation; (c) delivery; (d) exploitation; (e) installation; (f) command and control; (g) exfiltration. **S 11.9** - Financial institutions must ensure continuous monitoring and timely detection of anomalous activities, including: **(a)** establishing a Security Operations Center (SOC) with competent resources and necessary tools; **(b)** monitoring scope must cover all critical systems and supporting infrastructure; **(c)** conducting regular vulnerability assessments and penetration testing per Appendix 5. **S 11.10** - Financial institutions must establish processes to collect, analyse and evaluate cyber threat intelligence to detect cyber threats, data breaches, and misleading information about the institution online. **S 11.11** - Financial institutions must establish appropriate response processes to investigate and respond to flagged anomalous activities based on complexity level.	**Shared responsibility** **Customer responsibilities** - Establishing a Security Operations Center (SOC) - Implementing security controls - Conducting continuous monitoring of your AWS environments - Establishing processes - Implementing incident response procedures - Conducting regular vulnerability assessments and penetration testing of your instances and applications - Defining your operational model for security monitoring, incident detection, and response based on the AWS services you choose to use. **AWS responsibilities** - Security of the cloud infrastructure, including the host operating system, virtualization layer, and physical security of facilities. - Continuous monitoring of AWS infrastructure to detect unusual or unauthorized activities. - Vulnerability management of the underlying infrastructure. - Proactive monitoring of vendor flaws through newsfeeds and vendor websites. AWS Security teams monitor for new patches. *AWS services and resources that can help support this requirement:* *Monitoring and Detection Services* **Amazon CloudWatch** – Monitor applications, respond to system-wide performance changes, optimize resource utilization, and gain unified operational health visibility. Centralize logs from systems, applications, and AWS services. **AWS CloudTrail** – Monitor and record account activity across AWS infrastructure, capturing comprehensive history of changes for security and operational issue discovery and troubleshooting. **Amazon GuardDuty** – Continuously monitor for malicious activity and unauthorized behavior to protect AWS accounts and workloads. Provides threat detection using machine learning and threat intelligence. **AWS Security Hub** – Provides a comprehensive view of security alerts and security posture across AWS accounts, aggregating findings from multiple AWS services and third-party tools.	**SEC 10**: How do you anticipate, respond to, and recover from incidents? **SEC 4**: How do you detect and investigate security events? **SEC 1**: How do you securely operate your workload? **SEC 5**: How do you protect your network resources? **SEC 6**: How do you protect your compute resources? **OPS 10**: How do you manage workload and operations events? **OPS 8**: How do you utilize workload observability in your organization? **OPS 9**: How do you understand the health of your operations? **SEC 2**: How do you manage identities for people and machines? **SEC 3**: How do you manage permissions for people and machines?

Summary of requirements	AWS Considerations	Implementation
	AWS Config – Continually assess, audit, and evaluate configurations and relationships of resources on AWS, on-premises, and on other clouds. **AWS Config Rules** – Automate compliance checking and track configuration changes. *Threat Intelligence and Analysis* **Amazon Detective** – Analyze and visualize security data to rapidly investigate potential security issues or suspicious activities. **AWS Security Bulletins** – Stay updated on security announcements and vulnerabilities. *Response and Remediation* **AWS Systems Manager** – Automate operational tasks and manage AWS resources at scale. **AWS Lambda** – Automate responses to security events and anomalies. *Vulnerability Management* **Amazon Inspector** – Automated security assessment service to help improve security and compliance of applications deployed on AWS. *Network Security* **AWS WAF (Web Application Firewall)** – Protect web applications against common web exploits and bots that can affect availability, compromise security, or consume excessive resources. **AWS Shield** – Managed DDoS protection service. Standard tier is included automatically. Advanced tier is available for enhanced protection. **AWS Network Firewall** – Deploy network security across VPCs with managed firewall service. *Logging and Audit* **Amazon CloudWatch Logs** – Centralize logs for analysis, search, and archival. **AWS Artifact** – Access compliance reports and security controls documentation (SOC reports, ISO certifications, PCI DSS reports). *Health and Status Monitoring* **AWS Health Dashboard** – Personalized view of AWS service performance and availability, with proactive notifications for scheduled activities and events. *Support*	

Summary of requirements	AWS Considerations	Implementation
	AWS Support Plans – Access to security and operational guidance from AWS support engineers. Multiple tiers are available.	

Cyber Response and Recovery

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 11.12 Financial institutions must establish comprehensive cyber crisis management policies incorporating cyber-attack scenarios into overall crisis management, escalation processes, business continuity, and disaster recovery planning, including clear communication plans for stakeholders. **S 11.13** Financial institutions must establish and implement a comprehensive Cyber Incident Response Plan (CIRP) addressing: **(a)** Preparedness - Clear governance, reporting structure, roles/responsibilities of CERT, and invocation/escalation procedures; **(b)** Detection and analysis - Effective processes for identifying compromise points, assessing damage, and preserving forensic evidence; **(c)** Containment and eradication - Remedial actions to minimize damage, contain/remove threats, and resume operations; **(d)** Recovery - Multiple strategies including contingency plans for swift resumption and enhanced redundancy/resilience; and **(e)** Post-incident activity - Post-incident reviews with lessons learned and long-term risk mitigations. **S 11.14** Financial institutions must ensure CERT members are conversant with incident response plans and remain contactable at all times. **S 11.15** Financial institutions shall establish secure out-of-band communication infrastructure for internal/external stakeholders to ensure coordination if primary systems are compromised.	**Customer responsibility** - Crisis Management and Incident Response Planning - Communication and Coordination - Training and Preparedness - Testing and Validation - Insurance and Loss Provisions - Integration with Business Continuity *AWS services and resources that can help support this requirement:* *Incident Detection and Analysis* **AWS CloudTrail** – Discover and troubleshoot security and operational issues by capturing a comprehensive history of changes in your AWS accounts. **Amazon CloudWatch** – Monitor applications, respond to system-wide performance changes, optimize resource use, and get a unified view of operational health. **Amazon GuardDuty** – Continuously monitor for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. **AWS Security Hub** – Centralized security and compliance monitoring. **AWS Config** – Track, monitor, analyze, and audit events. Assess, audit, and evaluate configurations of your AWS resources. **AWS Config Rules** – Automated compliance checking. *Communication and Coordination* **AWS Personal Health Dashboard** – Personalized view of service performance and availability with proactive notifications. **AWS Health API** – Programmatic access to health events for integration with incident management systems. *Forensics and Evidence Preservation* **AWS CloudTrail** – Comprehensive audit logging for forensic analysis. **Amazon CloudWatch Logs** – Centralize logs from systems, applications, and AWS services for analysis. **AWS Systems Manager** – Automate operational tasks and maintain security compliance. *Recovery and Resilience*	**SEC 10**: How do you anticipate, respond to, and recover from incidents? **OPS 10**: How do you manage workload and operations events? **REL 13**: How do you plan for disaster recovery (DR)? **REL 12**: How do you test reliability? **OPS 11**: How do you evolve operations? **SEC 4**: How do you detect and investigate security events? **OPS 7**: How do you know that you are ready to support a workload? **OPS 9**: How do you understand the health of your operations?

Summary of requirements	AWS Considerations	Implementation
S 11.16 Financial institutions must conduct annual cyber drill exercises testing CIRP effectiveness and out-of-band communications with board, senior management, and third-party involvement. Results must be reported to the board timely. Test scenarios must include: **(a)** Effectiveness of escalation, communication, and decision-making for different incident impact levels; and **(b)** Readiness and effectiveness of CERT and third-party service providers in recovery. **S 11.17** Financial institutions shall review loss provision arrangements for cyber incident adequacy based on extreme adverse event scenarios. For cyber insurance adoption: **(a)** Ensure policy scope adequately covers information security events and liability exposures; **(b)** Understand policy terms regarding warranties, attestations, and responsibilities; reflect in crisis response procedures; ensure IT changes don't create coverage exclusions; and **(c)** Ensure policy obligations don't impair ability to act in best interest of institution and customers; manage conflicts arising from insurer's cost minimization objectives.	**AWS Backup** – Centralized backup service for AWS resources. **AWS Elastic Disaster Recovery** – Minimize downtime and data loss with fast, reliable recovery. **Multiple Availability Zones** – Deploy across multiple Availability Zones for high availability. **Multiple AWS Regions** – Geographic separation for disaster recovery. *Testing and Validation* **AWS Resilience Hub** – Assess and track application resilience. **AWS Fault Injection Service** – Test application behavior under stress conditions. *Documentation and Compliance* **AWS Artifact** – Access to compliance reports and certifications, including SOC 2 reports that contain incident management details. **AWS Security Bulletins** – Stay updated on security announcements. *Support* **AWS Support Plans** – Access to support engineers for operational issues and technical questions (Basic, Developer, Business, Enterprise).	

Cyber Reporting and Threat Information Sharing

WAF Pillars: Operational excellence (OPS), Security (SEC), Reliability (REL), Performance efficiency (PERF), Cost optimization (COST), and Sustainability (SUS)

Summary of requirements	AWS Considerations	Implementation
S 11.18 Financial institutions must notify the Bank of cyber incidents following requirements in: - Operational Risk Reporting – Part C - Business Continuity Management – Part C - Merchant Acquiring Services (paragraphs 19.25-19.26) - Other relevant Bank policy documents **S 11.19** Financial institutions must: Share cyber threat intelligence information with industry via relevant platforms (Bank, industry, or law enforcement) in compliance with data protection laws Allocate resources for industry-wide threat intelligence improvement initiatives **S 11.20** Financial institutions must collaborate and cooperate with relevant stakeholders and authorities to combat cyber threats.	**Customer responsibility** - Incident Notification to Regulators - Cyber Threat Intelligence Sharing - Stakeholder Collaboration - Incident Management Process *AWS services and resources that can help support this requirement:* *Incident Detection and Monitoring* **AWS CloudTrail**: Discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in your AWS account within a specified period of time **Amazon CloudWatch**: Monitor applications, respond to system-wide performance changes, optimize resource use, and get a unified view of operational health **Amazon GuardDuty**: Continuously monitor for malicious activity and unauthorized behavior to protect your AWS accounts and workloads **AWS Security Hub**: Provides a comprehensive view of security alerts and security posture across your AWS accounts **AWS Config**: Continually assess, audit, and evaluate the configurations and relationships of your resources *Incident Response and Analysis* **AWS Security Incident Response Guide**: Provides guidance on incident response processes and procedures **AWS Config Rules**: Track, monitor, analyze, and audit events to identify qualifying incidents *Monitoring and Alerting* **AWS Personal Health Dashboard**: Provides a personalized view into the performance and availability of services, displaying relevant and timely information to help you manage events in progress **AWS Security Bulletins**: Keep updated on security announcements *Logging and Audit Trail* **Amazon CloudWatch Logs**: Centralize logs from your systems, applications, and AWS services in a single, highly scalable service for analysis and investigation	**SEC 10**: How do you anticipate, respond to, and recover from incidents? **OPS 10**: How do you manage workload and operations events? **SEC 4**: How do you detect and investigate security events? **SEC 1**: How do you securely operate your workload? **OPS 9**: How do you understand the health of your operations?

Summary of requirements	AWS Considerations	Implementation
	Compliance and Reporting **AWS Artifact**: Access audit and compliance reports to support your regulatory reporting requirements *Additional Considerations* As part of the shared security responsibility model, you and AWS both perform security events monitoring. You can use the tools listed previously to track, monitor, analyze, and audit events. If these tools identify an event that is analyzed and determined to be an incident requiring regulatory notification, you must trigger your incident management process and follow your established procedures for notifying the Bank and sharing threat intelligence with relevant stakeholders. Establish clear procedures and workflows that integrate these AWS services with your regulatory reporting obligations and threat intelligence sharing platforms.	

Document revisions

Date	Description
March 2026	First publication.