AWS User Guide to Hong Kong Monetary Authority's (HKMA) Practice Guide on Cloud Adoption

February 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 requirements in HKMA's Practice Guide on Cloud Adoption 10

- Principle 1A: Cloud strategy and governance framework 12
- Principle 1B: Board and senior management oversight 14
- Principle 1C: Cloud record management 16
- Principle 1D: Stakeholder engagement 18
- Principle 2A: Pre-adoption risk assessment 20
- Principle 2B: Provider selection and due diligence 22
- Principle 2C: Ongoing reviews of risk assessment frameworks and CSP 24
- arrangements 24
- Principle 3A: CSP contractual arrangements and safeguards 26
- Principle 3B: Subcontracting management 27
- Principle 3C: Shared responsibility model 28
- Principle 3D: Standards and certification assurance 29
- Principle 4A: Cloud resilience 30
- Principle 4B: Business continuity planning 32
- Principle 4C: Portability and interoperability 34
- Principle 4D: Exit strategy 36
- Principle 5A: Cloud security framework 37
- Principle 5B: Secure architecture and deployment 39
- Principle 5C: Identity and access management 42

Principle 5D: Data classification and protection 45
Principle 5E: Data residency and regulatory assurance 47
Principle 6A: Cloud incident management and testing 49
Principle 7A: Integrated security monitoring 51
Principle 7B: Service performance and log management 53
Principle 8A: Workforce strategy and resource management 56
Principle 8B: Workforce training and competency development 58
Document revisions 60

Abstract

This document provides AWS customers in the financial services sector with guidance on addressing the Hong Kong Monetary Authority's (HKMA) Practice Guide on Cloud Adoption. It serves as a practical reference for Authorized Institutions (AIs) seeking to understand how AWS services, security controls, and compliance programs can support their regulatory obligations when adopting cloud services. It explains the AWS Shared Responsibility Model, which delineates security responsibilities between AWS (security *of* the cloud) and customers (security *in* the cloud).

The core of the document maps HKMA's eight principles and their sub-principles to relevant AWS services and Well-Architected Framework best practices. For each principle, the guide clarifies customer responsibilities, identifies applicable AWS services and tools, and references specific Well-Architected Framework practices.

Introduction

In January 2026, the HKMA issued a Practice Guide on Cloud Adoption to support Authorized Institutions (AIs) in implementing cloud technology within their banking operations. Superseding the Guidance on Cloud Computing published in 2022, this Practice Guide reflects the HKMA's commitment to supporting "progressively incorporating cloud technology" within AIs' operations in a prudent manner and promoting "responsible innovation" through an interactive and iterative supervisory approach.

The Practice Guide responds to significant developments in the banking sector, where cloud-related projects now represent approximately 80% of all reportable technology outsourcing initiatives, with one-third to one-half involving critical banking systems. AIs have progressively adopted increasingly sophisticated cloud models, including private, public, hybrid, and multi-cloud environments. Drawing from over 70 supervisory engagements with AIs and international best practices, the HKMA has determined that expanded guidance is necessary to address this evolving landscape.

The Practice Guide employs a dual-layered framework consisting of: (1) high-level principles derived from relevant Supervisory Policy Manual modules, and (2) good practices observed through supervisory work that provide actionable implementation guidance. This structure ensures supervisory expectations remain current and applicable across diverse cloud adoption scenarios while offering practical reference points for AIs.

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 HKMA's Practice Guide on Cloud Adoption. 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.

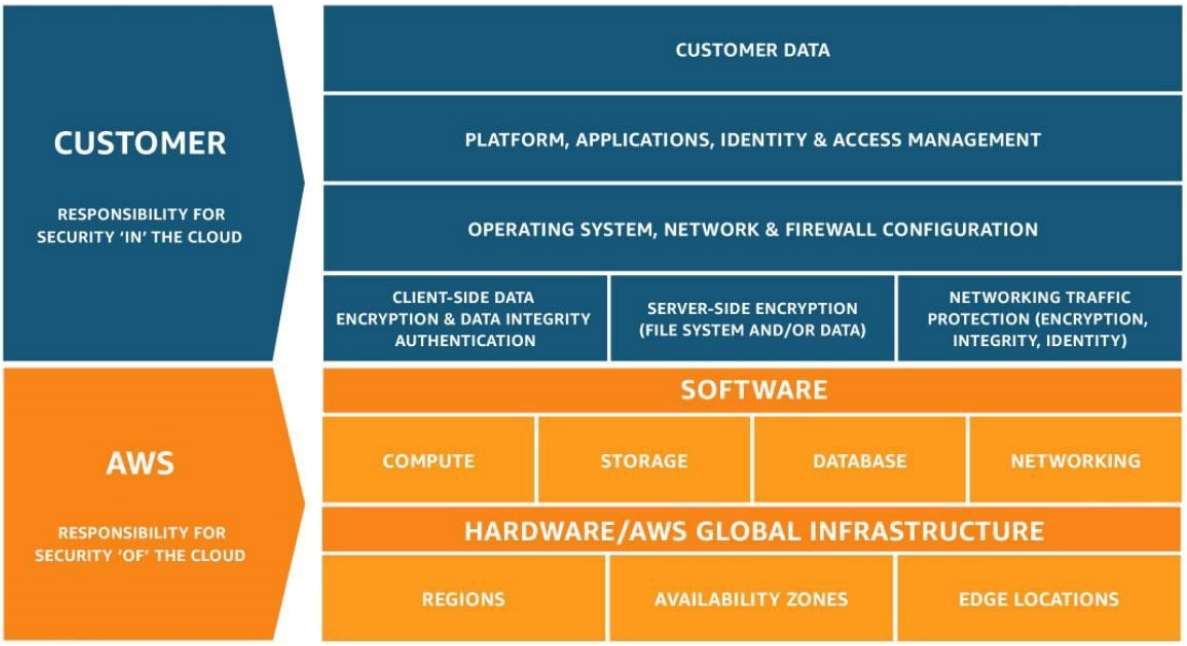


Figure 1 – The AWS Shared Responsibility Model

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 42001**: ISO/IEC 42001 is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organizations. It is designed for entities providing or utilizing AI-based products or services, ensuring responsible development and use of AI systems. For more information or to download the AWS ISO 42001 certification, see the ISO 42001 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 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.

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 supervised by the HKMA, 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, conduct 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 in HKMA's Practice Guide on Cloud Adoption.

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.
- 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 requirements in HKMA's Practice Guide on Cloud Adoption

The following sections list key technical and operational requirements identified in HKMA's Practice Guide on Cloud Adoption 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 Expectations:** Summarizes the requirements and good practices identified in the HKMA's Practice Guide on Cloud Adoption. This is not the original text of the Practice Guide on Cloud Adoption, but a summary. Please note that this summary reflects the dual-layered structure of the HKMA Practice Guide on Cloud Adoption, which distinguishes between mandatory regulatory requirements and recommended good practices. The HKMA **Principles** (expressed using directive language such as "should") represent requirements that Authorized Institutions should apply in a manner proportionate to their risk profile. The **Good Practices** (typically presented as bullet points in the original guide) are recommendations that institutions should adopt where appropriate for their specific circumstances. Both the Principles and Good Practices are summarized in the Summary of Expectations.
- **AWS Considerations:** Explains the considerations for addressing the requirements identified in the Practice Guide on Cloud Adoption. 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.

Principle 1A: Cloud strategy and governance framework

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

Summary of Expectations	AWS Considerations	Implementation

AIs must establish a Board-approved cloud strategy aligned with strategic objectives, risk appetite, operational resilience targets, and regulatory obligations. Group entities should adapt overarching strategies to local priorities while maintaining timely group communication channels.
 	
A cloud governance framework must translate strategy into practice through defined oversight, roles, responsibilities, and risk management proportionate to cloud adoption materiality. The framework should integrate with enterprise-wide risk and resilience frameworks, adapt to different deployment models, and undergo periodic Board and senior management review.
 	
Review cloud strategy on defined cycles (e.g., annually and post-material changes) for alignment with business priorities, risk exposures, and regulations.
Document linkages between cloud strategy and other enterprise strategies (digital transformation, outsourcing, cybersecurity) with visible dependencies.
Develop cloud adoption policy specifying approval processes, implementation responsibilities, model-specific controls (access management, data protection, monitoring), and compensating measures for CSP responsibilities (external and intra-group).
Utilize post-migration reviews, incident analyses, and cross-project reviews to refine governance and strengthen future adoption.
	Customer responsibility
	
	- Defining and maintaining their cloud strategy and governance framework
	- Board-level oversight and approval
	- Policy development and documentation
	- Periodic review and continuous improvement
	- Integration with enterprise frameworks
	- Coordination
	
	AWS services and resources that can help support this requirement:
	- AWS maintains comprehensive documentation on its services, IT control environment, security controls, and compliance programs available through:
	  - AWS website and whitepapers
	  - AWS Artifact for compliance reports and certifications (SOC 1, SOC 2, SOC 3, ISO 27001, ISO 27017, ISO 27018, ISO42001 PCI DSS)
	- AWS manages security of the cloud
	- AWS provides detailed information about:
	  - Service capabilities and technical documentation
	  - Control environment and security measures
	  - Compliance certifications and attestations
	
	Governance and Oversight Tools
	AWS Organizations - Centrally manages and governs multiple AWS accounts, implement service control policies, and enforce organizational standards
	AWS Control Tower - Sets up and governs a secure, multi-account AWS environment based on best practices
	AWS Config - Assesses, audits, and evaluates configurations of AWS resources for compliance with internal policies
	
	Risk Management and Monitoring
	AWS Security Hub - Centralized view of security alerts and compliance status across AWS accounts
		OPS 1: How do you determine what your priorities are?
		OPS 2: How do you structure your organization to support your business outcomes?
		OPS 3: How does your organizational culture support your business outcomes?
		OPS 11: How do you evolve operations?

Summary of Expectations	AWS Considerations	Implementation
Benchmark governance arrangements against industry standards and regulatory expectations to identify enhancement gaps.	**AWS CloudTrail** - Monitors and records account activity for governance, compliance, and operational auditing **Amazon CloudWatch** - Monitors applications, responds to system-wide performance changes, and maintain operational health visibility **AWS Trusted Advisor** - Provides real-time guidance to help provision resources following AWS best practices *Compliance and Audit Support* **AWS Artifact** - On-demand access to AWS compliance reports, certifications, and security documentation (SOC reports, ISO certifications, PCI DSS reports) **AWS Audit Manager** - Continuously audits AWS usage to simplify risk assessment and compliance with regulations *Architecture and Best Practices* **AWS Well-Architected Framework** - Consistent approach to evaluate architectures across six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability **AWS Well-Architected Tool** - Reviews workloads against AWS best practices and identify areas for improvement *Documentation and Knowledge Resources* **AWS Documentation** - Comprehensive technical documentation for all AWS services **AWS Compliance Programs** - Information on certifications, attestations, laws, regulations, and frameworks **AWS Whitepapers** - Including "Overview of Amazon Web Services" and security-focused guidance **AWS Training and Certification** - Resources to help ensure staff have appropriate knowledge to manage AWS services	

Principle 1B: Board and senior management oversight

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

Summary of Expectations	AWS Considerations	Implementation
The Board and senior management must exercise effective ongoing oversight of cloud initiatives based on the approved cloud strategy and governance framework, ensuring active management of cloud-related risks per defined roles and responsibilities. Senior management implements the cloud strategy through adequate resource allocation, operational controls, and regular Board reporting. They should also promote open communication and workforce engagement via visible leadership and behaviors that foster alignment and resilience. **Affirm ultimate responsibility** for cloud-related risks with Board and senior management through documentation in charters, terms of reference, governance manuals, risk policies, and performance objectives/KPIs. **Establish governance structures** for effective cloud oversight, including committees, working groups, or designated functions with clear mandates coordinating cloud activities across business, risk, and technology domains. **Embed technical expertise** within governance and risk functions to support informed decision-making and ensure cloud risks are understood, assessed, and managed continuously. **Establish structured reporting** on cloud adoption using analysis tools (risk assessments, concentration dashboards) tracking key indicators: adoption progress, availability, concentration exposures, incidents, risk indicators, and compliance, with clear escalation of significant issues to Board and senior management.	**Customer responsibility** - Risk Management and Monitoring - Reporting and Transparency - Resource Allocation and Controls - Compliance and Audit *AWS services and resources that can support these requirements* - Comprehensive information on AWS services and IT control environment through whitepapers, reports, certifications, and third-party attestations - Independent assurance reports available through AWS Artifact for oversight of AWS global infrastructure - Financial statements of Amazon.com, Inc. (including AWS sales and income) available from the SEC or Amazon's Investor Relations website *Monitoring and Reporting Tools* **AWS CloudTrail** – Monitors and records account activity across AWS infrastructure, providing audit trails for governance oversight **Amazon CloudWatch** – Centralizes logs and monitor systems for operational health and performance metrics **AWS Config** – Continually assesses, audits, and evaluates configurations and relationships of resources **AWS Security Hub** – Provides comprehensive security posture visibility and compliance status **AWS Health Dashboard** – Personalized view of service availability and performance for reporting to senior management *Risk Assessment and Compliance Tools* **AWS Audit Manager** – Facilitates audits and continuous compliance assessments **AWS Trusted Advisor** – Provides best practice recommendations across multiple categories **Amazon GuardDuty** – Continuous security monitoring for threat detection	**OPS 1**: How do you determine what your priorities are? **OPS 2**: How do you structure your organization to support your business outcomes? **OPS 3**: How does your organizational culture support your business outcomes? **COST 1**: How do you implement cloud financial management? **COST 2**: How do you govern usage? **OPS 9**: How do you understand the health of your operations? **SEC 1**: How do you securely operate your workload? **COST 3**: How do you monitor usage and cost?

Summary of Expectations	AWS Considerations	Implementation
Promote transparency and awareness through visibility of cloud developments in senior communications, reinforcing governance and risk culture via internal channels (town halls, newsletters), and ensuring consistent communication of priorities and expectations institution-wide.	**AWS Artifact** – On-demand access to AWS security and compliance reports for Board-level oversight *Governance and Control Tools* **AWS Organizations** – Centrally manages and governs multiple AWS accounts with policy-based controls **AWS Identity and Access Management (IAM)** – Controls user and programmatic access with granular policies **AWS Control Tower** – Sets up and governs secure, multi-account AWS environments Architecture and Best Practices **AWS Well-Architected Framework** – Provides consistent approach to evaluate architectures across six pillars (operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability) **AWS Resilience Hub** – Assesses and improves application resilience *Support and Expertise* **AWS Support Plans** – Access to support engineers for operational and technical guidance (multiple tiers available) **AWS Training and Certification** – Resources to build technical expertise within governance functions *Recommendations* - Use AWS Artifact to access independent audit reports (SOC 1, SOC 2, SOC 3, ISO 27001, ISO 27017, ISO 27018, PCI DSS) that can support Board-level reporting on AWS control effectiveness - Implement comprehensive monitoring using AWS CloudTrail, CloudWatch, Security Hub, and Config to provide the data needed for regular Board and senior management reporting - Use AWS Well-Architected Framework to establish governance standards and assess cloud deployments against best practices - Establish clear responsibility matrices documenting which aspects of cloud operations are customer vs. AWS responsibilities, ensuring no ambiguity in accountability to the Board	

Principle 1C: Cloud record management

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

Summary of Expectations	AWS Considerations	Implementation

Effective oversight and risk management of cloud initiatives require maintaining complete, accurate, and current records of AI cloud resources and arrangements to support monitoring, incident management, planning, decision-making, and regulatory compliance.
 	
Cloud Asset Inventory: Maintain current inventory of applications, data repositories, infrastructure, and outsourced services. Scope and detail should match service model and management responsibility. Include criticality ratings, ownership, prompt updates for changes, and retain decommissioned arrangement records for risk monitoring, incident response, and audits.
Function Registry: Document all outsourced and cloud-supported functions (critical and non-critical), including function description/purpose, data type/sensitivity, CSP identity, processing/storage location, CSP legal jurisdiction, governing law, and subcontracting details where contractually available.
Registry Enhancement: Document application/system interdependencies, maintain configuration records, and regularly validate internal inventories against CSP-provided information for accuracy and completeness.
	Customer responsibility
	
	- Maintaining an up-to-date inventory of cloud assets
	- Maintaining a registry of outsourced and cloud-supported functions
	- Defining their governance, risk assessment, and operational process models for managing systems, databases, and services
	- Documenting application and system interdependencies and maintaining reliable configuration records
	- Choosing AWS Regions where content is stored and processed, maintaining control over data location and residency
	
	AWS services and resources that can help support this requirement:
	- Transparency on infrastructure and services through comprehensive documentation, whitepapers, and compliance reports
	- Independent third-party audit reports and certifications available through AWS Artifact, including:
	  - SOC 1, SOC 2, and SOC 3 reports
	  - ISO 27001, 27017, 27018, and 22301 certifications
	  - PCI DSS compliance reports
	  - Details about more than 2,600 security controls
	- Clear regional infrastructure information with AWS Regions and Availability Zones, though specific data center locations remain confidential for security purposes
	- Commitment to data sovereignty: AWS doesn't move or replicate customer content outside of chosen AWS Regions without customer agreement, except as necessary to comply with law
	
	Asset Inventory and Configuration Management
	AWS Config – Continuously assess, audit, and evaluate the configurations and relationships of resources on AWS, on-premises, and on other clouds. Provides configuration history and change tracking.
	AWS Systems Manager Inventory – Collects metadata about instances and the software installed on them, helping maintain an inventory of AWS resources.
		SEC 1: How do you securely operate your workload?
		SEC 7: How do you classify your data?
		COST 4: How do you decommission resources?
		OPS 4: How do you implement observability in your workload?
		REL 6: How do you monitor workload resources?
		COST 2: How do you govern usage?
		COST 3: How do you monitor usage and cost?

Summary of Expectations	AWS Considerations	Implementation
	AWS Resource Groups and Tag Editor – Organizes and manages AWS resources using tags, enabling categorization by criticality, ownership, environment, or other custom attributes. *Monitoring and Tracking* **AWS CloudTrail** – Monitors and records account activity across AWS infrastructure, providing a comprehensive audit trail of API calls, resource changes, and user actions. Logs can be retained for compliance and audit purposes. **Amazon CloudWatch** – Centralizes logs from systems, applications, and AWS services. Monitor resources and applications in real time and retain logs for historical analysis. **AWS Organizations** – Manages multiple AWS accounts centrally, with the ability to track resources across the organization and apply policies consistently. *Compliance and Audit Support* **AWS Artifact** – On-demand access to AWS security and compliance reports, certifications, and attestations to support audit and compliance reviews. **AWS Audit Manager** – Continuously audits AWS usage to simplify risk assessment and compliance with regulations and industry standards. Automates evidence collection and helps maintain audit-ready reports. **AWS Security Hub** – Provides a comprehensive view of security and compliance status AWS services and resources that can support these requirements	

Principle 1D: Stakeholder engagement

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

Summary of Expectations	AWS Considerations	Implementation
Cloud governance should be transparent and inclusive, engaging all relevant stakeholders within an AI to ensure business, technology, operations, risk, legal, and compliance perspectives are considered, fostering AI-wide buy-in and coherent cross-functional decision making. **Create a stakeholder engagement plan** defining which teams participate at each cloud adoption stage, including coordination processes and communication channels. **Conduct regular multi-disciplinary forums** to share cloud initiatives, risk assessments, and incident lessons, with clear documentation of input and agreed actions. **Use structured tools** (stakeholder matrices, consultation logs) to document stakeholder input in cloud decisions and communicate feedback. **Require documented sign-off** from all relevant functions for material cloud decisions (new platforms, critical workload migrations, exit planning), proportionate to their roles. **Conduct periodic stakeholder surveys** or feedback sessions to assess governance inclusiveness and effectiveness, using results for process refinement.	**Customer responsibility** - Defining Governance Structure - Establishing Communication Channels - Documenting Decision-Making - Implementing Review Mechanisms - Maintaining Transparency *AWS services and resources that can help support this requirement:* - Documentation and Resources: We provide comprehensive documentation, whitepapers, and guidance on cloud adoption best practices through resources such as: - AWS Well-Architected Framework - AWS Cloud Adoption Framework - Overview of Amazon Web Services whitepapers - Compliance Information: We make available independent third-party audit reports and certifications through AWS Artifact, enabling stakeholders to evaluate our control environment. - Support Services: We offer support plans and account management services to facilitate communication and coordination with customer stakeholders. **AWS Organizations**: Enables centralized governance and management across multiple AWS accounts, supporting structured oversight and policy enforcement across different business units and stakeholder groups. **AWS Control Tower**: Provides a framework for setting up and governing a secure, multi-account environment, with built-in governance guardrails. **AWS CloudTrail**: Captures comprehensive audit logs of account activity, providing transparency and accountability for stakeholder review and governance oversight. **AWS Config**: Continuously assesses, audits, and evaluates resource configurations, supporting compliance monitoring and stakeholder reporting. **AWS Security Hub**: Provides a comprehensive view of security and compliance status across AWS accounts, facilitating cross-functional visibility.	**OPS 1**: How do you determine what your priorities are? **OPS 2**: How do you structure your organization to support your business outcomes? **OPS 3**: How does your organizational culture support your business outcomes? **COST 1**: How do you implement cloud financial management? **SEC 1**: How do you securely operate your workload?

Summary of Expectations	AWS Considerations	Implementation
	AWS Artifact: Offers on-demand access to compliance reports and certifications, enabling stakeholders to review our security and compliance posture. **Amazon CloudWatch**: Enables monitoring and logging capabilities that support operational transparency and stakeholder oversight. **AWS Health Dashboard**: Provides personalized views of service availability and events, supporting proactive communication with stakeholders. **AWS Trusted Advisor**: Offers recommendations across multiple categories (cost optimization, security, performance, and so on) that can inform stakeholder discussions. **AWS Audit Manager**: Helps automate evidence collection for audits, supporting stakeholder engagement in compliance activities. *Additional Considerations* - You can clearly communicate the AWS Shared Responsibility Model to all stakeholders to ensure understanding of the delineation between AWS and customer responsibilities. - Customers can access AWS Training and Certification resources to make sure stakeholders have appropriate knowledge and understanding of AWS services and governance capabilities.	

Principle 2A: Pre-adoption risk assessment

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

Summary of Expectations	AWS Considerations	Implementation
AIs must conduct pre-adoption risk assessments commensurate with the nature, scale, complexity and criticality of intended cloud adoption, covering: (I) general technology risks, and (ii) cloud-specific considerations. Key assessment factors include: data location, jurisdictional/regulatory requirements, service provider reliance and supply chain dependencies, multi-tenancy arrangements, concentration risk from limited CSPs, and reduced control in SaaS models. The assessment enables informed decisions about cloud adoption readiness and required risk mitigations. **Structured assessment tools** - Use decision trees/whitelists to identify appropriate cloud services and deployment options based on risk, resilience, and transition/exit feasibility. **Internal capability assessment** - Evaluate AI's capacity to manage and oversee cloud arrangements, ensuring adequate resources, expertise, and governance processes exist. **Standardized risk assessment template** - Mandate comprehensive templates covering: (i) operational dependencies/resilience; (ii) security safeguards; (iii) legal/regulatory requirements; (iv) contractual protections; (v) reputational implications. Templates require governance review and endorsement before implementation. **Existing service dependency review** - Map current CSP reliance, subcontractors, and	**Customer responsibility** - Conducting comprehensive pre-adoption risk assessments - Defining your governance, risk assessment, and operational process models - Assessing internal capabilities - Evaluating data location and jurisdictional requirements - Assessing concentration risk - Reviewing existing cloud dependencies (if applicable) - Conducting scenario exercises - Evaluating SaaS-specific risks - Establishing multi-disciplinary governance review processes *AWS services and resources that can help support this requirement:* *Assessment and Planning Tools:* **AWS Well-Architected Framework** – Helps evaluate architectures against six pillars (operational excellence, security, reliability, performance efficiency, cost optimization, sustainability) **AWS Pricing Calculator** – Enables cost modeling and estimation before adoption *Governance and Control Services:* **AWS Organizations** – Manages multiple accounts and enforce policies across the organization **AWS Account Management** – Specifies which AWS Regions can be used for each account **AWS Identity and Access Management (IAM)** – Controls access to AWS services and resources *Monitoring and Compliance Services:* **AWS Artifact** – Accesses compliance reports and certifications (SOC 1/2/3, ISO 27001/27017/27018, PCI DSS, and so on) **AWS Audit Manager** – Facilitates audits and continuous compliance assessment **AWS Security Hub** – Centralized security and compliance view	**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? **OPS 3**: How does your organizational culture support your business outcomes? **SEC 7**: How do you classify your data? **REL 10**: How do you use fault isolation to protect your workload? **REL 13**: How do you plan for disaster recovery (DR)?

Summary of Expectations	AWS Considerations	Implementation
interdependencies. Use scenario exercises to assess how additional adoption could increase dependence and whether resulting risks are acceptable. **Jurisdictional/regulatory evaluation** - Review data/service locations and assess alignment with data protection and regulatory requirements before adoption. **SaaS-specific risk assessment** - Consider reduced control, limited audit access, CSP reporting reliance, and ensure clear data extraction/portability procedures. **Multi-disciplinary governance review** - Require involvement from business, technology, operations, risk, legal, and compliance functions with documented approval of conditions/mitigations before CSP selection.	**AWS Config** – Assesses, audits, and evaluates resource configurations **AWS Trusted Advisor** – Best practice recommendations **AWS CloudTrail** – Tracks account activity and API usage **Amazon CloudWatch** – Monitors resources and applications *Security Services:* **AWS Key Management Service (KMS)** – Manages encryption keys **AWS CloudHSM** – Hardware-based key storage **Amazon GuardDuty** – Threat detection service *Resilience and Business Continuity:* **AWS Resilience Hub** – Assesses and improves application resilience **Multiple Availability Zones** – Deploys across independent failure zones **Multiple AWS Regions** – Geographic distribution for disaster recovery *Data Transfer and Portability:* **AWS Database Migration Service** – Migrate databases in and out of AWS *Documentation and Guidance:* **AWS Compliance Programs webpage** – Information on certifications and attestations **AWS Customer Success website** – Case studies and references **AWS Security Bulletins** – Security announcements and updates **AWS Health Dashboard** – Service availability and personalized health information **Data Privacy Center** – Information on data privacy at AWS	

Principle 2B: Provider selection and due diligence

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

Summary of Expectations	AWS Considerations	Implementation
AIs must conduct robust evaluation and due diligence when shortlisting cloud vendors to ensure secure, reliable service delivery compliant with laws and regulations. Key Requirements: - Apply clear, documented, risk-based criteria - Ensure due diligence depth is proportionate to function criticality - Use systematic evaluation referencing industry frameworks and independent assurance - Employ consistent methodology leveraging recognized certifications, audit reports, and third-party assessments **Documented Framework**: Maintain evaluation criteria, scoring methods, and residual risk thresholds **Evidence-Based Approach**: - Verify certification scope/relevance for intended service model (IaaS, PaaS, SaaS) - Assess subcontracting arrangements, especially cross-boundary/multi-tiered structures - Review legal/regulatory environment of CSP operations and data locations for jurisdictional risks - Assess resilience using metrics (uptime, incidents, root cause analysis) and client references - Verify CSP security/data protection meets AI's standards via certifications and third-party assurance **Risk-Based Selection Criteria**: Cover (i) financial soundness; (ii) resources/expertise; (iii) operational resilience; (iv) security/data protection; (v) incident response; (vi) business continuity; (vii)	**Customer responsibility** - Due Diligence Framework and Evaluation Process - Evidence-Based Assessment Activities - Selection Criteria Definition *AWS services and resources that can help support this requirement:* *Compliance and Assurance Validation* **AWS Artifact**: Compliance reporting portal providing on-demand access to: - AWS SOC 1, SOC 2, and SOC 3 reports - ISO certifications (27001, 27017, 27018, 27701, 22301) - PCI DSS compliance reports - Details about more than 2,600 security controls - Reports from accreditation bodies across geographies and compliance verticals *Performance and Availability Monitoring* **AWS Health Dashboard**: Provides up-to-the-minute information on service availability in AWS Regions worldwide with personalized views **AWS Service Level Agreements (SLAs)**: Published online for all paid, generally available services **AWS Security Bulletins**: Website for staying updated on security announcements *Operational Monitoring and Assessment* **Amazon CloudWatch**: Monitors applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health **AWS CloudTrail**: Discovers and troubleshoots security and operational issues by capturing comprehensive history of changes **Amazon GuardDuty**: Continuously monitors for malicious activity and unauthorized behavior **AWS Config**: Continually assesses, audits, and evaluates configurations and relationships of resources **AWS Security Hub**: Centralized view of security and compliance status	**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?

Summary of Expectations	AWS Considerations	Implementation
subcontracting; (viii) regulatory compliance; (ix) data residency; (x) strategic alignment **Evaluation Team**: Include subject matter experts from business, technology, operations, risk, legal, and compliance	*Architecture and Best Practices Guidance* **AWS Well-Architected Framework**: Helps evaluate architectures against six pillars (operational excellence, security, reliability, performance efficiency, cost optimization, sustainability) **AWS Trusted Advisor**: Provides recommendations following AWS best practices *Support and Expert Consultation* **AWS Support Plans**: Four tiers available that allow you to contact support engineers for operational issues or technical questions *Documentation and Information Resources* **AWS Documentation**: Comprehensive technical documentation for all services **AWS Compliance Programs webpage**: Full list of certifications, attestations, and compliance programs **AWS Customer Success website**: Customer references and case studies **AWS Whitepapers**: Including "Overview of Amazon Web Services" and security-focused whitepapers *Additional considerations* - Use AWS Artifact as the primary source for validating AWS's control environment through independent third-party audit reports and certifications - Review AWS Financial Statements available through SEC filings and Amazon Investor Relations to assess financial soundness and long-term viability - Engage with AWS Representatives to obtain specific information about capabilities, subcontracting arrangements, and contractual frameworks - Use AWS Well-Architected Framework to make sure that AWS services align with organizational requirements - Reference AWS Customer Success Stories and case studies from similar financial institutions to validate operational track record - Establish monitoring using AWS native services (CloudWatch, CloudTrail, Security Hub) to continuously validate service quality and security posture post-selection	

Principle 2C: Ongoing reviews of risk assessment frameworks and CSP arrangements

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

Summary of Expectations	AWS Considerations	Implementation
Cloud arrangements require continuous monitoring as they evolve in scope, technology, and risk profile. AIs must conduct periodic reviews—not one-off assessments—to verify initial assumptions, evaluate CSP's security/compliance/financial status, and ensure alignment with risk appetite and regulatory obligations. Review frequency should match arrangement criticality and occur after significant incidents or material changes. The AI's risk assessment framework and due diligence methodology must also undergo periodic review and updates to reflect changes in business models, technology, regulations, threat landscape, and lessons from incidents, testing, industry practices, and supervisory feedback. **Schedule recurring risk assessments** (annually minimum for critical services) covering CSP certification, compliance, financial soundness, resilience, and risk posture. **Conduct ad-hoc reassessments after material events:** service disruptions, regulatory/audit findings, or emerging risk alerts. **Re-perform due diligence** when deficiencies arise or when entering/renewing CSP arrangements, considering change materiality.	**Customer responsibility** - Defining and maintaining governance, risk assessment, and operational process models for managing systems, databases, and services. - Conducting periodic reviews and assessments of cloud deployments in line with regulatory guidelines, circulars, and frameworks. - Scheduling recurring risk assessments - Performing ad-hoc reassessments following material events - Re-performing due diligence reviews when deficiencies are identified or when entering into or renewing arrangements - Continuously monitoring the CSP and complying with various regulatory, legal, and technical requirements notified by regulators or government authorities. - Maintaining an updated inventory of all services contracted with external companies, clearly determining those that are strategic and high risk. - Incorporating operational risk reports for the Board of Directors regarding actions carried out to manage outsourcing risks, including changes in the risk profile of suppliers. *AWS services and resources that can help support this requirement:* *Monitoring and Assessment Services:* **AWS Audit Manager** – Facilitates continuous auditing and automated evidence collection **AWS Security Hub** – Provides comprehensive security posture assessment and continuous compliance checks **AWS Config** – Continually assesses, audits, and evaluates configurations and relationships of resources **AWS Trusted Advisor** – Provides real-time guidance to help provision resources following AWS best practices **AWS Resilience Hub** – Helps assess and track application resilience	**OPS 11**: How do you evolve operations? **OPS 9**: How do you understand the health of your operations? **SEC 1**: How do you securely operate your workload? **OPS 10**: How do you manage workload and operations events? **SEC 10**: How do you anticipate, respond to, and recover from incidents?

Summary of Expectations	AWS Considerations	Implementation
	Continuous Monitoring Services: **Amazon CloudTrail** – Monitors and records account activity across AWS infrastructure **Amazon CloudWatch** – Centralizes logs and monitors applications for system-wide performance changes **Amazon GuardDuty** – Continuously monitors for malicious activity and unauthorized behavior **AWS Health Dashboard** – Provides personalized view of service availability and performance *Compliance and Reporting:* **AWS Artifact** – Provides on-demand access to AWS security and compliance reports, certifications, and attestations **AWS Well-Architected Framework** – Provides consistent approach to evaluate architectures against six pillars including security, reliability, and operational excellence *Additional Resources:* **AWS Support Plans** – Provides access to support engineers for operational issues and technical questions **AWS Security Bulletins** – Keeps you updated on security announcements *Additional considerations* - Use AWS Artifact regularly to access updated compliance reports and certifications to validate AWS's continued compliance standing. - Implement automated monitoring using AWS Config, Security Hub, and CloudWatch to enable continuous assessment of your cloud environment. - Review AWS financial information periodically through Amazon's Investor Relations portal to assess financial soundness. - Use the AWS Well-Architected Framework to periodically review and assess your architecture against AWS best practices and make sure alignment with evolving regulatory expectations.	

Principle 3A: CSP contractual arrangements and safeguards

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

Summary of Expectations	AWS Considerations	Implementation
AIs must establish clear, enforceable contracts with CSPs that include: (i) Audit and access rights for AI oversight (ii) HKMA supervisory access to cloud data and risk controls (iii) Safeguards for subcontracting (see Principle 3B) AIs should review contracts for fitness-for-purpose. **Contract elements to include:** - Defined scope, roles, responsibilities, deliverables, and monitoring mechanisms **Service level agreements (SLAs):** - Measurable indicators - Monitoring, reporting, remedial actions, and breach consequences **Rights and obligations:** - Incident notification channels - Termination rights and conditions - Exit support - Business continuity/disaster recovery testing, data retention and insurance coverage expectations - Security, confidentiality, regulatory compliance, data use restrictions, and data protection provisions - Governing law, jurisdiction, financial obligations, and data location commitments - Minimum notice period (e.g., 12 months) for critical service discontinuation **Review CSP standard terms** during procurement /renewal to identify gaps **Establish CSP cooperation expectations for audits**: timely responses, record access, expert designation, and third-party report clarification	**Customer responsibility** - Defining and maintaining contractual arrangements, governance, risk assessment, and operational process models *AWS services and resources that can help support this requirement:* **AWS Financial Services Addendum** – Provides contractual terms designed for enabling financial institutions to comply with applicable regulatory requirements *Compliance and Assurance* For assurance over AWS global infrastructure, institutions can rely on independent assurance made available at no charge through AWS Artifact We provide access to security and compliance reports from independent third-party auditors We maintain certifications including SOC 1, SOC 2, SOC 3, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 22301, and PCI DSS *SLAs* We offer SLAs for paid, generally available services AWS SLAs are published online and specify measurable availability targets	**OPS 1**: How do you determine what your priorities are? **OPS 2**: How do you structure your organization to support your business outcomes? **REL 12**: How do you test reliability? **REL 13**: How do you plan for disaster recovery (DR)? **SEC 1**: How do you securely operate your workload? **SEC 10**: How do you anticipate, respond to, and recover from incidents? **OPS 9**: How do you understand the health of your operations? **OPS 11**: How do you evolve operations? **SEC 4**: How do you detect and investigate security events? **SEC 7**: How do you classify your data? **SEC 8**: How do you protect your data at rest?

Principle 3B: Subcontracting management

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

Summary of Expectations	AWS Considerations	Implementation
Contractual provisions must extend beyond the AI-CSP relationship to cover subcontracting and downstream service providers. CSPs should remain contractually liable for subcontractor performance and compliance. AIs should retain notification, approval, and objection rights over material subcontracting arrangements and secure enforceable commitments ensuring equivalent resilience, security, data protection, and regulatory obligations across all third-party tiers. AIs must implement effective oversight arrangements for CSPs' subcontractor engagement.	**Customer responsibility** - Defining governance and contractual requirements for their operational model, including requirements for subcontractor management and oversight - Establishing policies and procedures governing subcontracting activities *AWS services and resources that can help support this requirement:* **AWS Financial Services Addendum**: Provides contractual terms enabling banking institutions to comply with applicable subcontracting requirements and regulatory obligations **AWS Artifact**: On-demand access to AWS compliance reports and certifications, including SOC 1, SOC 2, and SOC 3 reports, ISO 27001, ISO 27017, ISO 27018 certifications, PCI DSS compliance reports, details about the AWS control environment and subcontractor management.	Not applicable

Principle 3C: Shared responsibility model

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

Summary of Expectations	AWS Considerations	Implementation
AIs should establish and maintain a shared responsibility model with CSPs that clearly delineates: CSP's responsibility: "security of the cloud" AI's responsibility: "security in the cloud" The model must define responsibilities across different service models (IaaS, PaaS, SaaS), allocate control ownership to avoid gaps/overlaps, verify CSP capabilities, and be regularly reviewed as services, technologies, or risks evolve. **Document responsibilities across IaaS, PaaS, and SaaS**, distinguishing CSP's "security of the cloud" from AI's "security in the cloud," keeping mappings current. **Specify shared controls** (e.g., monitoring, recovery, key management) in terms of execution and validation where responsibility overlaps. **Embed agreed responsibilities** into AI's internal policies to guide staff, ensuring records are updated to reflect changes in services, risks, or technology. **Assess CSP capability periodically** through independent assurance reports, certifications, audits, or performance indicators. **Apply risk-based approach to identify gaps/residual risks**, ensuring review scope and frequency match arrangement criticality and exposures remain within approved risk tolerance.	**Customer responsibility** - Defining and Documenting the Shared Responsibility Model - Embedding Responsibilities into Internal Policies - Risk-Based Assessment and Verification - Service-Specific Responsibilities *AWS services and resources that can help support this requirement:* *Compliance and Assurance Resources* **AWS Artifact**: On-demand access to AWS compliance reports and certifications, including SOC 1, SOC 2, and SOC 3 reports, ISO 27001, ISO 27017, ISO 27018 certifications, PCI DSS compliance reports, details about more than 2,600 security controls. *Frameworks and Documentation* **AWS Well-Architected Framework** – Helps evaluate architectures against six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability **AWS Shared Responsibility Model Documentation** – Clearly defines the division of responsibilities **AWS Financial Services Addendum** – Provides contractual terms enabling financial institutions to comply with applicable regulatory requirements	**SEC 1**: How do you securely operate your workload? **OPS 2**: How do you structure your organization to support your business outcomes? **OPS 3**: How does your organizational culture support your business outcomes? **SEC 3**: How do you manage permissions for people and machines? **SEC 10**: How do you anticipate, respond to, and recover from incidents? **OPS 7**: How do you know that you are ready to support a workload? **REL 8**: How do you implement change?

Principle 3D: Standards and certification assurance

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

Summary of Expectations	AWS Considerations	Implementation
AIs must require CSPs to demonstrate compliance with recognized international and national standards proportionate to outsourced workload criticality. Certifications should be valid, relevant, and independently issued by accredited bodies. When certifications are unavailable, insufficient, or outdated, AIs should use alternative assurance through third-party assessments or equivalent measures to ensure CSP controls meet regulatory and internal requirements. **Benchmark CSP practices against industry frameworks** to validate control adequacy and consistency across service and deployment models. **Review CSP certifications/attestations** for authenticity, independence, scope, coverage, and validity—confirming they are current, accredited, relevant to services used, and cover applicable regions, workloads, and data.	**Customer responsibility** - Evaluating CSP Certifications and Standards - Accessing and Reviewing Compliance Documentation - Defining Governance and Risk Assessment - Contractual Requirements *AWS services and resources that can help support this requirement:* **AWS Financial Services Addendum** – Provides contractual terms enabling financial institutions to comply with applicable regulatory requirements *AWS Artifact* - Automated compliance reporting portal available in AWS Management Console - Provides on-demand access to AWS security and compliance documents - Includes SOC reports, PCI reports, and certifications from accreditation bodies - Helps you review and download reports and details about security controls - Available at no additional charge *AWS Compliance Programs* - Comprehensive information available at AWS Compliance Programs webpage - Covers certifications and attestations, laws and regulations, and alignment frameworks - Provides details on scope, validity, and independent assessor information	**SEC 1**: How do you securely operate your workload? **OPS 2**: How do you structure your organization to support your business outcomes?

Principle 4A: Cloud resilience

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

Summary of Expectations	AWS Considerations	Implementation
AIs must design cloud arrangements for resilience to support critical operations under severe scenarios. Resilience should match workload criticality, using geographic and infrastructure redundancy to minimize single points of failure and enable recovery/failover. AIs should mitigate dependencies on individual CSPs or geographic locations to address concentration and geopolitical risks, with stricter safeguards for critical workloads. **Design critical workloads across multiple, geographically dispersed, independently powered data centres** with resilient interconnections and seamless failover to absorb disruptions without interruption. **Integrate on-premises and public cloud environments** to diversify resilience, provide fallback capacity, and enhance flexibility. **Apply risk-based resilience measures**, using stronger approaches (multiple CSP regions/availability zones) for critical operations, with regular reviews for alignment with objectives and regulations. **Utilize CSP-native resilience features** (automatic recovery, dynamic scaling) while ensuring proper configuration, testing, and monitoring. **Reduce single-CSP reliance** through hybrid or multi-cloud strategies prioritizing critical workloads, supported by consistent governance, unified security policies, and cross-provider capable staff.	**Customer responsibility** - Designing and implementing resilient architectures for workloads across multiple AWS Regions and Availability Zones based on criticality. - Implementing contingency planning, training, and testing for systems hosted on AWS. - Defining governance, risk assessment, and operational process models for managing systems, databases, and services. - Choosing AWS Regions where content is stored. They can replicate and back up content in more than one AWS Region. - Configuring and testing resilience features, including automatic recovery and dynamic scaling. *AWS services and resources that can help support this requirement:* *Resilience and High Availability* **AWS Regions and Availability Zones** – Deploy across multiple Availability Zones within a Region or across multiple Regions for geographic diversity. **Amazon CloudWatch** – Monitors applications, respond to system-wide performance changes, and optimize resource utilization. **AWS Auto Scaling** – Automatically adjusts capacity to maintain steady, predictable performance. **Elastic Load Balancing** – Automatically distributes incoming traffic across multiple targets. *Disaster Recovery and Backup* **AWS Backup** – Centralized backup service to automate and manage backups across AWS services. **AWS Elastic Disaster Recovery** – Minimizes downtime and data loss with fast, reliable recovery. *Multi-Region and Hybrid Capabilities*	**REL 3**: How do you design your workload service architecture? **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? **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)? **REL 1**: How do you manage Service Quotas and constraints? **REL 2**: How do you plan your network topology? **REL 6**: How do you monitor workload resources? **OPS 1**: How do you determine what your priorities are? **OPS 10**: How do you manage workload and operations events?

Summary of Expectations	AWS Considerations	Implementation
	Amazon Route 53 – Highly available and scalable DNS with health checking and failover capabilities. **AWS Direct Connect** – Establish dedicated network connections from on-premises to AWS. *Monitoring and Testing* **AWS Resilience Hub** – Assesses, tracks, and improves application resilience. **AWS Health Dashboard** – Personalized view into the performance and availability of AWS services. **AWS CloudTrail** – Tracks user activity and API usage for audit and compliance. **AWS Config** – Assesses, audits, and evaluates configurations of AWS resources. *Architecture Guidance* **AWS Well-Architected Framework** – Reliability pillar provides guidance on building resilient architectures. **AWS Architecture Center** – Reference architectures and best practices for disaster recovery.	**SUS 1**: How do you select Regions for your workload?

Principle 4B: Business continuity planning

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

Summary of Expectations	AWS Considerations	Implementation
AIs must implement comprehensive business continuity management frameworks aligned with strategic objectives, risk appetite, and regulatory obligations. This includes continuity plans for cloud services, backup/recovery arrangements, and CSP resilience assessments to mitigate downtime, data loss, and disruptions to critical operations. Disaster recovery arrangements require regular oversight, periodic testing, and CSP capability assessments. **Establish proportionate business continuity and fallback arrangements** for cloud workloads based on criticality and risk tolerance, defining RTOs and RPOs aligned with approved tolerance levels and incorporating alternative service options. **Integrate CSP continuity capabilities** into AI-wide planning by reviewing CSP documentation (business continuity summaries, disaster recovery plans, testing evidence) and aligning testing schedules. **Assess CSP disaster recovery effectiveness** through practical recovery evidence and test results rather than certifications alone, verifying reliability under severe scenarios (cyberattacks, system failures, data centre unavailability). **Conduct joint continuity drills** with CSPs where practicable to validate arrangements and identify improvements. **Review business continuity framework regularly** and after major changes in workloads, CSP arrangements, or risk factors to ensure continued alignment.	**Customer responsibility** - Properly implementing contingency planning, training, and testing for their systems hosted on AWS - Defining recovery time objectives (RTOs) and recovery point objectives (RPOs) based on business impact analysis (BIA) and risk impact analysis (RIA) consistent with the criticality of workloads - Establishing their own business continuity and disaster recovery plans that integrate cloud service provider (CSP) capabilities - Conducting regular testing of recovery plans at least annually, including disaster scenarios - Implementing robust continuity plans *AWS services and resources that can help support this requirement:* *Disaster Recovery and Business Continuity* **Multiple AWS Regions** – Deploy across geographic Regions for disaster recovery Availability Zones – Deploy across multiple Availability Zones within Regions for high availability **AWS Backup** – Centralized backup service for AWS resources **AWS Elastic Disaster Recovery** – Minimizes downtime and data loss with fast, reliable recovery *Monitoring and Testing* **AWS Health Dashboard** – Personalized view of service performance and availability with proactive notifications **Amazon CloudWatch** – Monitors applications, responds to performance changes, and gain operational visibility **AWS CloudTrail** – Tracks account activity and changes for audit and compliance *Data Replication and Recovery* **Amazon S3 Cross-Region Replication** – Automatically replicates data across Regions	**REL 13**: How do you plan for disaster recovery (DR)? **REL 12**: How do you test reliability? **REL 11**: How do you design your workload to withstand component failures? **REL 9**: How do you back up data? **OPS 7**: How do you know that you are ready to support a workload? **REL 10**: How do you use fault isolation to protect your workload? **OPS 10**: How do you manage workload and operations events?

Summary of Expectations	AWS Considerations	Implementation
	Amazon RDS Multi-AZ Deployments – Automatic failover for database workloads **AWS Database Migration Service** – Migrates databases with minimal downtime *Resilience Assessment* **AWS Resilience Hub** – Assesses and tracks application resilience against disruptions **AWS Well-Architected Framework** – Reliability pillar provides best practices for resilient architectures *Documentation and Compliance* **AWS Artifact** – Access to SOC 2 reports documenting AWS business continuity testing and controls **AWS Service Level Agreements (SLAs)** – Documented commitments for service availability *Data Transfer for Recovery* **AWS DataSync** – Automates data transfer between on-premises and AWS	

Principle 4C: Portability and interoperability

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

Summary of Expectations	AWS Considerations	Implementation
AIs should design cloud workloads to be portable (migrate between environments with minimal modification) and interoperable (exchange information reliably across systems/CSPs) based on criticality. This enables secure, efficient migration of workloads and data in response to strategic changes, disruptions, or severe scenarios. Consider during CSP selection and maintain throughout arrangements. **Open standards adoption** - Use open standards for data formats, APIs, and software interfaces to enable seamless migration across cloud or on-premises environments. **Operationalize through technology** - Implement containerization, orchestration, standardized integration layers, API gateways, and cross-environment compatibility testing for smooth deployment and recovery. **Verify CSP mechanisms** - Ensure CSPs provide validated backup, migration, and data recovery mechanisms; confirm configurations support secure, efficient workload movement. **Integrate into lifecycle** - Maintain and validate interoperability tools during patching, upgrades, and retirement to keep interfaces, data exchange, and migration pathways compatible and secure. **CSP-neutral designs** - Use distributed architectures and interoperable components to minimize vendor lock-in and preserve multi-environment operation capability.	**Customer responsibility** - Designing workloads for portability. - Defining governance, risk assessment, and operational model based on the AWS services and products in use. - Maintaining control over content and data, including choosing which AWS Regions to store content and how to configure their environments. - Implementing and validating portability mechanisms. - Integrating interoperability maintenance into system lifecycle activities, including patching, upgrades, and system retirement. - Implementing contingency planning, training, and testing for your systems hosted on AWS. *AWS services and resources that can help support this requirement:* *Migration and Portability Services* **AWS Database Migration Service** – Migrates databases from AWS services to on-premises databases or between environments. **Cloud Storage on AWS** – Various storage services that help with data transfer and portability. *Multi-Region and High Availability* **AWS Regions and Availability Zones** – Deploy across multiple geographic Regions and Availability Zones for resilience and portability. **Data replication capabilities** – Replicate and back up content across multiple AWS Regions. *Monitoring and Validation* **AWS Config** – Continually assesses, audits, and evaluates configurations and relationships of resources. **Amazon CloudWatch** – Monitors applications and system-wide performance. **AWS CloudTrail** – Monitors and records account activity for compliance validation.	**REL 3**: How do you design your workload service architecture? **PERF 1**: How do you select appropriate cloud resources and architecture patterns for your workload? **REL 13**: How do you plan for disaster recovery (DR)? **REL 9**: How do you back up data? **REL 8**: How do you implement change? **REL 12**: How do you test reliability? **PERF 3**: How do you store, manage, and access data in your workload?

Summary of Expectations	AWS Considerations	Implementation
	Architecture Frameworks **AWS Well-Architected Framework** – Provides a consistent approach to evaluate architectures with a focus on operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. *Backup and Recovery* **Cross-Region replication** – Replicates data across multiple Regions for disaster recovery.	

Principle 4D: Exit strategy

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

Summary of Expectations	AWS Considerations	Implementation
AIs must establish viable exit strategies to ensure cloud-dependent operations can continue if a cloud arrangement terminates. Exit plans should include objectives, risk indicators, termination procedures, migration arrangements, and defined triggers, with periodic reviews and testing for feasibility. **Assessment and planning**: Conduct business impact and technical assessments to determine transition timelines, costs, and required skillsets; identify substitute CSPs, in-house alternatives, and migration tools/standards. **Advance strategy design**: Develop exit strategies for all cloud services, especially those supporting critical operations, detailing objectives, success criteria, roles, responsibilities, costs, and timelines to enable disruption-free service termination and transfer. **Structural constraints**: Address limitations like intra-group dependencies or cross-boundary arrangements; identify alternatives such as transitional service agreements, hybrid/multi-cloud configurations, or on-premises fallback environments. **Regular testing**: Test exit plan feasibility through desktop reviews, walkthroughs, or staff readiness checks; conduct stressed exit testing where appropriate to reconcile backup data and identify hidden operational risks.	**Customer responsibility** - Exit planning and strategy development - Data portability and retrieval - Testing and validation - Contractual provisions *AWS services and resources that can help support this requirement:* *Data migration and transfer services* **AWS Database Migration Service** – Web service to migrate databases from AWS services to on-premises databases. **Cloud Storage on AWS** – Various services facilitate data transfer during exit. *Multi-Region and hybrid architecture support* **AWS Regions and Availability Zones** – Enable customers to replicate and back up content in more than one AWS Region, supporting multi-cloud and hybrid configurations. *Business continuity support* **Multiple Availability Zones** – Design independent failure zones to support transitional service arrangements. **Cross-Region Replication** – Enables backup and disaster recovery configurations during exit transitions.	**REL 13**: How do you plan for disaster recovery (DR)? **REL 12**: How do you test reliability? **REL 9**: How do you back up data? **OPS 7**: How do you know that you are ready to support a workload? **REL 11**: How do you design your workload to withstand component failures? **REL 8**: How do you implement change? **OPS 2**: How do you structure your organization to support your business outcomes?

Principle 5A: Cloud security framework

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

Summary of Expectations	AWS Considerations	Implementation
AIs must establish and maintain a comprehensive cloud security framework for safeguarding cloud assets. The framework should define security measures, assurance requirements, and provide direction for secure architecture, IAM, data governance, cryptographic key management, and related controls. It must apply consistently across all cloud models, scale to system criticality, and undergo ongoing oversight to address emerging threats and technological changes. **Governance**: Establish clear roles, responsibilities, and accountability for cloud security aligned with broader governance frameworks, supported by formal documentation and periodic assurance reviews. **Risk-based structure**: Address distinct risk characteristics of different cloud deployment and service models (public, private, hybrid, multi-cloud, IaaS, PaaS, SaaS) with clear security control expectations for each context. **Consistency and maintenance**: Design framework to ensure consistent, effective cloud security controls across all environments, including hybrid and multi-cloud configurations, with periodic reviews and updates for evolving risks and regulations.	**Customer responsibility** - Establishing Governance and Framework - Security Control Implementation - Framework Maintenance and Updates - Monitoring and Assurance *AWS services and resources that can help support this requirement:* *Governance and Compliance* **AWS Artifact** – Access security and compliance reports, including SOC 1, SOC 2, SOC 3, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 22301, and PCI DSS reports. **AWS Organizations** – Centrally manages and governs AWS accounts. **AWS Control Tower** – Sets up and governs secure, multi-account AWS environments. *Security Assessment and Monitoring* **AWS Security Hub** – Views security alerts and compliance status across AWS accounts from a central location. **AWS Config** – Assesses, audits, and evaluates configurations of AWS resources. **AWS Audit Manager** – Continuously audits AWS usage to simplify risk and compliance assessment. **AWS Trusted Advisor** – Gets real-time guidance to provision resources following AWS best practices. *Identity and Access Management* **AWS Identity and Access Management (IAM)** – Controls user and programmatic access to AWS services and resources with granular policies. **AWS IAM Identity Center** – Centrally manages workforce access to multiple AWS accounts and applications. *Monitoring and Logging*	**SEC 1**: How do you securely operate your 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 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? **SEC 11**: How do you incorporate and validate security properties of apps during design, development, and deployment lifecycle? **SEC 4**: How do you detect and investigate security events? **OPS 11**: How do you evolve operations?

Summary of Expectations	AWS Considerations	Implementation
	AWS CloudTrail – Monitors and records account activity across AWS infrastructure. **Amazon CloudWatch** – Monitors applications, respond to system-wide performance changes, and gain a unified view of operational health. **Amazon GuardDuty** – Continuously monitors for malicious activity and unauthorized behavior. *Data Protection and Encryption* **AWS Key Management Service (AWS KMS)** – Creates and manages cryptographic keys. **AWS CloudHSM** – Uses hardware-based key storage for regulatory compliance. **AWS Secrets Manager** – Rotates, manages, and retrieves secrets. *Network Security* **AWS WAF** – Protects against common web exploits with a web application firewall. **AWS Shield** – Gets DDoS protection (Standard and Advanced tiers). **AWS Network Firewall** – Deploy network security across VPCs. *Architecture and Best Practices* **AWS Well-Architected Framework** – Uses a consistent approach to evaluate architectures across six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. **AWS Resilience Hub** – Prepares and protects applications from disruptions. *Multi-Region and Multi-Account Support* **AWS Regions and Availability Zones** – Deploys across multiple geographic locations for resilience. **AWS Account Management** – Specifies which AWS Regions can be used for each AWS account. *Contractual Framework* **AWS Financial Services Addendum** – Provides contractual terms enabling financial institutions to comply with applicable regulatory requirements.	

Principle 5B: Secure architecture and deployment

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

Summary of Expectations	AWS Considerations	Implementation
AIs must design resilient cloud architectures using modern security practices across infrastructure and application lifecycles, including network design, configuration management, software security, and backup/recovery. **Network Design and Segmentation** - Implement clear segmentation between development, testing, and production environments with strict tenant isolation to prevent cross-environment compromise and lateral attacks. **Application and API Security** - Apply secure development disciplines including threat analysis and security principles throughout cloud application lifecycles. - Protect APIs and micro-services via least-privilege access, strong authentication, monitoring, timely decommissioning, and service discovery safeguards. **Workload and Container Security** - Use hardened configurations for VMs and containers, limit unnecessary components, and continuously monitor for vulnerabilities. - Secure container environments by restricting orchestrator access, controlling registries, and deploying only trusted images. - Adopt immutable infrastructure to minimize configuration drift and enable consistent redeployment. **Automated Deployment and Configuration Management** - Use Infrastructure as Code (IaC) and CI/CD pipelines to standardize deployments, reduce manual	**Customer responsibility** - Network Design and Segmentation - Application and API Security - Workload and Container Security - Configuration and Patch Management - Backup and Recovery *AWS services and resources that can help support this requirement:* *Network Security and Segmentation* **Amazon VPC (Virtual Private Cloud)** – Enables network isolation and segmentation. **AWS Organizations** – Helps manage multiple accounts with segregation. **AWS Security Groups and Network ACLs** – Control inbound and outbound traffic. *Identity and Access Management* **AWS Identity and Access Management (IAM)** – Controls user and programmatic access with granular policies. **AWS IAM Identity Center** – Centralized access management. **Multi-Factor Authentication (MFA)** – Strong authentication requirements. *Application and API Security* **AWS WAF (Web Application Firewall)** – Protects web applications against common exploits. **Amazon API Gateway** – Secure API management with authentication and authorization. **AWS Shield** – DDoS protection (Standard and Advanced tiers). *Container and Workload Security* **Amazon ECS (Elastic Container Service)** – Secure container orchestration. **Amazon EKS (Elastic Kubernetes Service)** – Managed Kubernetes with security controls. **Amazon ECR (Elastic Container Registry)** – Secure container image storage.	**SEC 1**: How do you securely operate your workload? **SEC 3**: How do you manage permissions for people and machines? **SEC 5**: How do you protect your network resources? **SEC 6**: How do you protect your compute resources? **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 9**: How do you back up data? **REL 12**: How do you test reliability? **REL 13**: How do you plan for disaster recovery (DR)? **SEC 2**: How do you manage identities for people and machines? **SEC 4**: How do you detect and investigate security events?

Summary of Expectations	AWS Considerations	Implementation
intervention, enforce duty segregation, and maintain integrity. - Deploy Policy as Code tools to automatically validate and enforce security compliance. **Cloud Security and Policy Enforcement** - Strengthen visibility, threat protection, and policy enforcement using native capabilities: CASB, CNAPP, CSPM, and CWPP. **Patch Management** - Implement structured patch management with clear AI-CSP responsibilities, ensuring thorough assessment, testing, controlled deployment, and synchronization across production and disaster-recovery environments. **Backup and Recovery** - Enforce technical controls including timely restoration, replication to alternate sites, and segregated/offline systems to minimize CSP-level failure exposure. - Conduct regular scenario-based testing to verify backup integrity and recoverability, with post-restoration security validation before service resumption.	**AWS Fargate** – Serverless container compute. *Configuration and Compliance Management* **AWS Config** – Continuously assesses, audits, and evaluates configurations. **AWS Systems Manager** – Centralized operational data and automation. **AWS Security Hub** – Comprehensive security posture management (CSPM capabilities). *Infrastructure as Code and Automation* **AWS CloudFormation** – Infrastructure as Code deployment. **AWS CDK (Cloud Development Kit)** – Defines cloud infrastructure using code. **AWS CodePipeline** – CI/CD automation. **AWS CodeBuild** – Builds and tests code with security scanning. *Monitoring and Threat Detection* **AWS CloudTrail** – Tracks user activity and API usage. **Amazon CloudWatch** – Monitors applications and infrastructure. **Amazon GuardDuty** – Intelligent threat detection (CWPP capabilities). **AWS Security Hub** – Centralized security findings (CNAPP capabilities). **Amazon Detective** – Security investigation and analysis. **Amazon Macie** – Data security and privacy protection. *Patch Management* **AWS Systems Manager Patch Manager** – Automates patching of managed instances. **Amazon Inspector** – Automated vulnerability management. *Backup and Recovery* **AWS Backup** – Centralized backup management. **Amazon S3** – Durable object storage with versioning and replication. **AWS Elastic Disaster Recovery** – Application recovery orchestration. **Amazon RDS automated backups** – Database backup and recovery. *Policy Enforcement* **AWS Organizations Service Control Policies (SCPs)** – Policy as Code enforcement. **AWS IAM Access Analyzer** – Validate access policies. **AWS Control Tower** – Governance and compliance automation. *Encryption and Data Protection*	**OPS 4**: How do you implement observability in your workload? **REL 6**: How do you monitor workload resources? **REL 8**: How do you implement change? **REL 10**: How do you use fault isolation to protect your workload?

Summary of Expectations	AWS Considerations	Implementation
	AWS Key Management Service (KMS) – Encryption key management. **AWS CloudHSM** – Hardware-based key storage. **AWS Certificate Manager** – SSL/TLS certificate management. **Amazon EBS encryption** – Volume encryption at rest. **Amazon S3 encryption** – Object encryption (SSE-S3, SSE-KMS, SSE-C). *Compliance and Audit Support* **AWS Artifact** – Access to compliance reports and certifications. **AWS Audit Manager** – Continuous audit readiness. **AWS Trusted Advisor** – Best practice recommendations. *Additional Resources* **AWS Well-Architected Framework** – Security Pillar provides best practices for secure architecture. **AWS Security Best Practices** – Comprehensive security guidance. **AWS Compliance Programs** – ISO 27001, SOC 2, PCI DSS and other certifications available through AWS Artifact. **Logical Separation on AWS whitepaper** – Details on tenant isolation. **AWS Security Incident Response Guide** – Incident management guidance.	

Principle 5C: Identity and access management

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

Summary of Expectations	AWS Considerations	Implementation
AIs must implement effective IAM arrangements ensuring only authorized users and system components access cloud resources at appropriate privilege levels. Frameworks should manage identities, entitlements, and privileges while enforcing segregation of duties, strong authentication, zero-trust principles, and applying to both internal and CSP environments. **Define and document cloud IAM roles and responsibilities**, including configuration rights, with clear accountability for each role. **Maintain comprehensive IAM policies for all cloud users** and components with regular reviews, requiring CSP alignment and implementing mitigating controls for gaps. **Enforce strong authentication for privileged access, including MFA** for management consoles and CSP administrative planes, using hardened endpoints and encryption. **Implement zero-trust principles** through least-privilege access, deny-by-default settings, micro-segmentation, continuous validation, and disciplined access lifecycle management proportionate to criticality. **Regularly rotate and secure credentials**, immediately deactivate unused credentials, and apply secure processes for credential management. **Implement continuous monitoring of user activities** with tamper-resistant audit trails and automated alerting for unauthorized or anomalous behavior.	**Customer responsibility** - Defining IAM Policies and Roles - Access Control Configuration - Authentication Requirements - Least Privilege Implementation - Access Lifecycle Management - Monitoring and Auditing - Governance Framework *AWS services and resources that can help support this requirement:* *Core Identity and Access Management* **AWS Identity and Access Management (IAM)** - Controls user and programmatic access to AWS services and resources. - Applies granular policies that assign permissions to users, groups, roles, or resources. - Enforces strong password practices including complexity requirements and MFA. - Supports federation with existing directory services. - Turn on secure access through roles, instance profiles, identity federation, and temporary credentials. **AWS Organizations** - Centrally manages and governs multiple AWS accounts. - Applies service control policies (SCPs) across accounts. - Denies access to operations outside specified AWS Regions. *Authentication and Access Control* **Multi-Factor Authentication (MFA)** - Requires MFA for privileged and sensitive access. - Support for hardware and virtual MFA devices. **AWS IAM Identity Center (successor to AWS Single Sign-On**) - Implements federated IAM solutions to unify identities across cloud and on-premises environments.	**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 4**: How do you detect and investigate security events?

Summary of Expectations	AWS Considerations	Implementation
Apply real-time control over privileged activities using granular entitlements, maker-checker functions, and PAM tools. **Adopt federated IAM solutions to unify identities across environments**, enhancing authentication through contextual checks (device, location, user-behavior). **Design IAM architecture for scalability and resilience** with automated lifecycle management and fault-tolerant identity services across deployment models.	- Turns on single sign-on access to multiple AWS accounts and applications. **AWS Directory Service** - Integrates with existing Microsoft Active Directory. - Supports federated identity management. *Privileged Access Management* **AWS Systems Manager Session Manager** - Provides secure access to EC2 instances without requiring open inbound ports. - Turn on auditable privileged access with session logging. **AWS Secrets Manager** - Securely stores, rotates, and manages credentials. - Automates credential rotation for supported services. **AWS Key Management Service (AWS KMS)** - Manages encryption keys with fine-grained access controls. - Support for customer managed keys with full control. *Monitoring and Auditing* **AWS CloudTrail** - Provides tamper-resistant audit trails of all API calls and user activities. - Turn on continuous monitoring of account activity across AWS infrastructure. - Captures comprehensive history of changes for security analysis. **Amazon CloudWatch** - Monitors and logs user access activities. - Sets up automated alerts for unauthorized or anomalous behavior. - Centralizes logs from systems, applications, and AWS services. **AWS Config** - Continuously assesses, audits, and evaluates configurations of AWS resources. - Tracks configuration changes and compliance status. - Implements automated compliance checks. **Amazon GuardDuty** - Continuously monitors for malicious activity and unauthorized behavior. - Detects anomalous access patterns and potential security threats. - Provides intelligent threat detection using machine learning. **AWS Security Hub** - Provides centralized view of security alerts and compliance status. - Aggregates findings from multiple AWS security services. - Automate compliance checks against security standards. *Access Control and Network Security* **AWS IAM Access Analyzer**	

Summary of Expectations	AWS Considerations	Implementation
	- Identify resources shared with external entities. - Validate that access policies grant only intended permissions. - Continuously analyze resource policies. **AWS Resource Access Manager (AWS RAM)** - Securely share resources across AWS accounts. - Implement fine-grained access controls for shared resources. **VPC Security Groups and Network ACLs** - Implement micro-segmentation and network-level access controls. - Enforce zero-trust network architecture principles. *Compliance and Governance* **AWS Artifact** - Access compliance reports and certifications (SOC 1, SOC 2, ISO 27001, PCI DSS). - Review security controls and attestations from independent auditors. - Validate implementation and effectiveness of AWS security controls. **AWS Audit Manager** - Automate evidence collection for audits. - Continuously assess controls against compliance frameworks. - Generate audit-ready reports. **AWS Control Tower** - Set up and govern multi-account AWS environments. - Implement preventive and detective guardrails. - Automate account provisioning with security baselines. *Additional Security Services* **AWS Certificate Manager** - Manage SSL/TLS certificates for secure communications. - Support end-to-end encryption requirements. **AWS WAF (Web Application Firewall)** - Protect web applications with granular access controls. - Implement contextual access controls based on request attributes.	

Principle 5D: Data classification and protection

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

Summary of requirements	AWS Considerations	Implementation
AIs are ultimately responsible for cloud-hosted data security and integrity regardless of cloud arrangement type. AIs must systematically classify data by sensitivity and business importance, implementing appropriate layered security controls throughout the data lifecycle, including encryption, key management, data loss prevention, and secure disposal. **Classify data by sensitivity and criticality** (especially confidential business and customer data); apply appropriate protection measures including de-identification, pseudonymisation, or anonymisation. **Encrypt data at rest, in transit, in use, and in backup** using strong, current cryptographic algorithms and appropriate key lengths; regularly review cryptographic standards. **Establish secure, encrypted channels** for cloud migration and operations. **Maintain comprehensive cryptographic key management policies** covering justification, generation, assignment, rotation, backup, deletion, and lifecycle review. **Exercise independent encryption key control through BYOE, BYOK, or HSMs where practicable**; avoid key reuse; ensure centralized, scalable key management integrated with IAM. **Extend data loss prevention and rights management to cloud data**; apply network segmentation and endpoint protection for devices accessing cloud services. **Regularly evaluate CSP multi-tenancy and logical separation controls** through technical testing at	**Customer responsibility** - Data Classification and Control - Encryption Implementation - Key management - Data Loss Prevention and Access Control *AWS services and resources that can help support this requirement:* *Encryption Services* **Data at rest encryption capabilities available in most AWS services**, including: - Amazon Elastic Block Store (Amazon EBS) - Amazon Simple Storage Service (Amazon S3) - Amazon Relational Database Service (Amazon RDS) - Amazon Redshift - Amazon ElastiCache - AWS Lambda - Amazon SageMaker *Key Management Services* **AWS Key Management Service (AWS KMS)** – Flexible key management options that let you choose whether to have AWS manage the encryption keys or keep complete control over your own keys. **AWS CloudHSM** – Dedicated, hardware-based cryptographic key storage that lets you help satisfy compliance requirements and secure encryption keys in a service backed by FIPS-validated HSMs. *Data Protection Services* **Server-side encryption (SSE) for Amazon SQS** – Encrypted message queues for the transmission of sensitive data. **Amazon EBS encryption** – AWS-managed disk encryption for additional data protection.	**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 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 5**: How do you protect your network resources? **SEC 6**: How do you protect your compute resources?

Summary of requirements	AWS Considerations	Implementation
compute, storage, and network layers to prevent cross-tenant data exposure. **Ensure secure data disposal** by working with CSPs on robust erasure and proper hardware/virtual resource disposal, supported by written confirmations, periodic audits, and final assurance of irreversible data removal.	*Access Control and Identity Management* **AWS Identity and Access Management (IAM)** – Control user and programmatic access to AWS services and resources with granular policies. **AWS Organizations** – Centralized access control and policy management. **AWS CloudTrail** – Comprehensive logging and monitoring of account activity. *Monitoring and Compliance* **AWS Config** – Continually assess, audit, and evaluate the configurations and relationships of resources. **Amazon CloudWatch** – Centralize logs from systems, applications, and AWS services for monitoring and analysis. **AWS Security Hub** – Centralized security and compliance monitoring. **Amazon GuardDuty** – Continuous security monitoring for malicious activity. *Network Security* **Amazon EC2 firewall** – Resides within the hypervisor layer for instance isolation. **Network segmentation** capabilities through Virtual Private Cloud (VPC) configurations. *Documentation and Compliance* **AWS Artifact** – On-demand access to security and compliance reports (SOC 1, SOC 2, SOC 3, ISO 27001, ISO 27017, ISO 27018, PCI DSS). **AWS Well-Architected Framework** – Guidance for building secure, high-performing, resilient, and efficient infrastructure. *Additional Considerations* **AWS Enterprise Agreement** – Provides contractual framework designed for financial institutions **Data Privacy** - AWS doesn't access or use your content for any purpose without your agreement. - AWS never uses your content or derives information from it for marketing or advertising purposes. - For information about data privacy at AWS, you can visit the Data Privacy Center website.	

Principle 5E: Data residency and regulatory assurance

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

Summary of requirements	AWS Considerations	Implementation
AIs must ensure data residency and regulatory compliance when selecting cloud storage/processing locations for customer data. This requires maintaining visibility of data locations within CSP infrastructures, assessing cross-border transfer risks, and managing subcontractor arrangements for legal compliance. **Jurisdictional reviews**: Conduct periodic reviews of cloud services to confirm data storage/processing arrangements comply with evolving data-residency laws, including monitoring legislative changes and engaging CSPs to validate locations align with approved regions. **Location visibility controls**: Establish technical/procedural controls to maintain visibility of actual data locations using CSP location APIs, security dashboards, or data-mapping automation, validated through periodic reviews or third-party audits. **Subcontracting risk assessment**: Assess data-related risks from subcontracting chains, particularly confidentiality and compliance risks where subcontractors operate in different jurisdictions, including evaluation of CSP due-diligence and transparency on data-handling arrangements. **Legal advice on transfers**: Obtain legal/specialist advice to assess cross-boundary data transfers, ensuring mechanisms like contractual clauses, transfer impact assessments, or certification schemes address applicable data protection and regulatory requirements.	**Customer responsibility** - Data Location Control and Visibility - Monitoring and Compliance - Subcontractor Management *AWS services and resources that can help support this requirement:* *Location Control and Visibility* **AWS Account Management** – Specify which AWS Regions can be used for each AWS account. For more information, see the AWS Account Management Reference Guide. **AWS Organizations** – Deny access to operations outside of specified AWS Regions. For more information, see the AWS Organizations User Guide. **AWS CloudTrail** – Set up alarms to notify you when AWS resources are launched in *Monitoring and Compliance* **AWS Config** – Continually assess, audit, and evaluate the configurations and relationships of resources on AWS, on premises, and on other clouds. **AWS Artifact** – On-demand access to security and compliance reports from AWS, including independent assurance over AWS global infrastructure. **AWS Audit Manager** – Facilitate audits of cloud deployments. **AWS Security Hub** – Centralized security and compliance monitoring. *Data Protection* **AWS Key Management Service (AWS KMS)** – Manage encryption keys with customer control options. **AWS CloudHSM** – Dedicated, hardware-based cryptographic key storage for compliance requirements. *Visibility and Tracking* **Amazon CloudWatch** – Monitor applications, respond to system-wide performance changes, and get a unified view of operational health.	**SUS 1**: How do you select Regions for your workload? **SEC 7**: How do you classify your data? **SEC 1**: How do you securely operate your workload? **SEC 8**: How do you protect your data at rest? **SEC 9**: How do you protect your data in transit? **OPS 1**: How do you determine what your priorities are? **OPS 4**: How do you implement observability in your workload?

Summary of requirements	AWS Considerations	Implementation
	AWS Personal Health Dashboard – Personalized view of the performance and availability of services with relevant and timely information. *Additional Guidance* - Additional detail about the general location of data centers is contained in the PCI-DSS report available through AWS Artifact. - For information about data privacy at AWS, visit the Data Privacy Center website. - You can access the AWS Global Infrastructure webpage for more information.	

Principle 6A: Cloud incident management and testing

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

Summary of requirements	AWS Considerations	Implementation
AIs must ensure incident response plans address cloud-related risks across all cloud environments (private, public, hybrid, multi-cloud). Plans should define actions for cloud disruptions including CSP outages, security breaches, and data access loss, aligned with broader incident and crisis management frameworks. Plans must specify responsibilities for escalation, decision-making, communication, and coordination with internal/external parties and CSPs to enable timely investigation, resolution, and regulatory reporting. AIs must fulfill all legal, regulatory, and contractual reporting obligations promptly with CSP support, ensuring transparent stakeholder communication. AIs should maintain plan effectiveness through regular reviews, testing, and updates based on lessons learned, system changes, and industry developments. **Align incident response with crisis management framework** via actionable mechanisms (joint escalation matrices, coordinated response structures, CSP contact points, consolidated dashboards). **Define objective escalation criteria** (breach severity, outage duration, reporting triggers) and decision owners for timely, consistent responses. **Map notification pathways and timeframes** for regulators, law enforcement, customers, and stakeholders using predefined templates.	**Customer responsibility** - Defining your incident response and crisis management framework - Establishing governance, risk assessment, and operational process models - Implementing incident detection and monitoring - Developing and maintaining incident response playbooks that include the CSP - Establishing notification pathways and communication protocols - Conducting regular testing of incident response plans - Regularly reviewing and updating procedures *AWS services and resources that can help support this requirement:* *Monitoring and Detection Services* **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 utilization, and get a unified view of operational health. CloudWatch centralizes logs from systems, applications, and AWS services. **Amazon GuardDuty** – Continuously monitor for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. **AWS Security Hub** – Get a comprehensive view of security alerts and compliance status across AWS accounts. **AWS Config** – Continually assess, audit, and evaluate the configurations and relationships of resources on AWS, on premises, and on other clouds. *Communication and Alerting Services* **AWS Personal Health Dashboard** – Get a personalized view into the performance and availability of services, see relevant and timely information to help manage events in progress, and receive proactive notification to help plan for scheduled activities. **AWS Health** – Monitor and record account activity and receive notifications about events that might affect AWS resources.	**SEC 10**: How do you anticipate, respond to, and recover from incidents? **OPS 10**: How do you manage workload and operations events? **REL 12**: How do you test reliability? **REL 13**: How do you plan for disaster recovery (DR)? **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 11**: How do you evolve operations? **SEC 4**: How do you detect and investigate security events?

Summary of requirements	AWS Considerations	Implementation
Maintain cloud-focused playbooks (CSP contacts, fallback arrangements, coordination steps for hybrid/multi-cloud environments) for rapid response. **Regularly assess CSP communication and escalation channel** performance for reliability and security. **Establish structured internal reporting workflows** and templates for consolidating incident information and ensuring accurate regulatory/stakeholder notifications. **Maintain current operational procedures and arrangements** (trained staff, validated contacts, tested channels) for effective notification execution. **Regularly test plans through scenario-based exercises** (breaches, outages, misconfigurations), involving CSPs in joint drills where applicable. **Update plans using test findings**, incident lessons, and industry insights to refine protocols and strengthen training.	**Amazon EventBridge** – Monitor and manage AWS Health events and trigger automated responses. *Incident Response and Forensics* **AWS Security Incident Response Guide** – Get guidance on incident response procedures and best practices. **AWS Systems Manager Incident Manager** – Prepare for and respond to incidents affecting AWS-hosted applications. *Compliance and Audit* **AWS Artifact** – Access AWS SOC 2 reports and other compliance documentation that detail AWS incident management controls and testing procedures. **AWS Audit Manager** – Continuously audit AWS usage to simplify risk assessment and compliance. *Support Services* **AWS Support Plans** – Get access to support engineers for operational issues or technical questions, with four tiers available for different levels of support during incidents. *Additional Guidance* **AWS Security Incident Response Guide** – For detailed guidance on building incident response capabilities **NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud** – For framework alignment **AWS Well-Architected Framework** – For operational excellence and security best practices **Disaster Recovery of Workloads on AWS: Recovery in the Cloud** – For recovery planning and testing approaches **AWS Enterprise Agreement** – Provides contractual framework designed for financial institutions	

Principle 7A: Integrated security monitoring

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

Summary of requirements	AWS Considerations	Implementation
AIs must conduct ongoing monitoring of CSP arrangements to detect security compromises timely. This requires implementing integrated security monitoring across cloud environments, consolidating data from multiple sources for timely alerts, centralized visibility, and proactive threat detection. Monitoring should cover key security and operational layers, extending to CSPs and subcontractors where feasible. SOC strategies should combine CSP and subcontractor monitoring data with the AI's own data for comprehensive analysis and timely incident response. Monitoring capabilities require regular evaluation and optimization for reliable, actionable alerts integrated into incident response processes. **Consolidate and correlate monitoring data from diverse sources** (activity logs, network flows, API audits, endpoint alerts, CSP alerts) into central SIEM platforms for near real-time cross-domain visibility. **Define monitoring coverage across all security layers** (network, workload, application, storage) with clear ownership assignments. **Integrate CSP monitoring data with internal logs** via secure APIs or cross-account pipelines for end-to-end cloud visibility. **Operationalize SOC workflows** with cloud-specific triage playbooks, automated alert enrichment, and predefined escalation criteria linked to incident response procedures. **Periodically calibrate monitoring rules**, detection logic, and alert thresholds with cloud engineers and	**Customer responsibility** - Defining and implementing your security monitoring strategy - Configuring and managing monitoring tools - Establishing Security Operations Center (SOC) workflows - Regularly calibrating monitoring rules, detection logic, and alert thresholds - Operationalizing monitoring outputs *AWS services and resources that can help support this requirement:* *Core Monitoring and Logging Services* **AWS CloudTrail** - Captures comprehensive history of API calls and account activity - Helps you discover and troubleshoot security and operational issues - Provides audit logs for compliance and governance **Amazon CloudWatch** - Centralized monitoring of applications, systems, and AWS services - Collects and tracks metrics, logs, and sets alarms - Provides system-wide visibility into resource utilization and operational health - Provides near real-time monitoring and alerting **Amazon CloudWatch Logs** - Centralizes logs from systems, applications, and AWS services - Helps you search, filter, and archive log data - Provides single, consistent flow of events ordered by time *Security Detection and Analysis* **Amazon GuardDuty** - Continuous security monitoring service - Detects malicious activity and unauthorized behavior - Protects AWS accounts and workloads - Provides threat intelligence and anomaly detection **AWS Security Hub** - Centralized security and compliance view	**SEC 4**: How do you detect and investigate security events? **SEC 10**: How do you anticipate, respond to, and recover from incidents? **OPS 8**: How do you utilize workload observability in your organization? **OPS 10**: How do you manage workload and operations events? **SEC 1**: How do you securely operate your workload? **OPS 4**: How do you implement observability in your workload?

Summary of requirements	AWS Considerations	Implementation
threat-intelligence teams to reduce false positives/negatives and align with evolving threats. **Use monitoring outputs to enhance operational procedures**, refine controls, and strengthen preventive measures through systematic integration into incident management and continuous improvement processes.	- Aggregates, organizes, and prioritizes security alerts - Consolidates findings from multiple AWS services and third-party tools - Provides comprehensive security posture management **AWS Config** - Continuously assesses, audits, and evaluates configurations - Tracks resource configuration changes - Provides compliance monitoring and security analysis *Additional Security Services* **AWS Audit Manager** - Facilitates continuous auditing of AWS usage - Automates evidence collection for compliance **AWS Trusted Advisor** - Provides real-time guidance on AWS best practices - Monitors security and performance **AWS Personal Health Dashboard** - Personalized view of service performance and availability - Proactive notifications for scheduled activities and events - Relevant and timely information for event management *Integration and Automation* **AWS Identity and Access Management (IAM)** - Controls user and programmatic access - Provides monitoring of authentication and authorization events **AWS Organizations** - Centralized management across multiple AWS accounts - Provides consolidated monitoring and governance	

Principle 7B: Service performance and log 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
Ongoing monitoring must cover service performance and log management beyond security. AIs should monitor SLA compliance, contractual obligations, and regulatory requirements for outsourced functions, including availability, reliability, and auditability through independent validation tools, while tracking CSP service updates and lifecycle events for risk assessment. For log management, AIs need cloud-specific approaches ensuring completeness, integrity, and availability of log data. Logs must provide visibility into user and system activities, including privileged operations, to support detection, investigation, and audit per regulatory requirements. **Use structured dashboards, automated analytics, and periodic reviews** to assess CSP performance trends, identify degradation, and escalate SLA breaches. **Deploy independent tools** (uptime monitoring, network measurement, log analytics platforms) to validate CSP dashboards and strengthen service assurance. **Maintain oversight of CSP operational updates and lifecycle events** (maintenance, modifications, disruptions, deprecations) for proactive risk assessment, including pre-change reviews and post-event reporting. **Establish comprehensive cloud-tailored log management** covering infrastructure, services, and privileged operations, with clear ownership for generation, collection, retention, and review.	**Customer responsibility** - Service performance monitoring - Log management *AWS services and resources that can help support this requirement:* *Service Performance Monitoring* **AWS Health Dashboard** - Provides personalized view into performance and availability of AWS services. - Displays relevant and timely information for managing events in progress. - Provides proactive notification for scheduled activities. - Provides up-to-the-minute information on service availability across AWS Regions. **Amazon CloudWatch** - Monitors applications and responds to system-wide performance changes. - Collects and tracks metrics, monitors log files, and sets alarms. - Provides unified view of operational health. - Provides system-wide visibility into resource utilization and application performance. - Supports custom performance metrics and thresholds. **AWS Trusted Advisor** - Provides real-time guidance to help provision resources following AWS best practices. - Checks for service quotas and performance optimization opportunities. **AWS Service Level Agreements (SLAs)** - Documented commitments for service availability. - For more information, see AWS Service Level Agreements. *Log Management* **AWS CloudTrail** - Records account activity across AWS infrastructure. - Provides full control over storage, analysis, and remediation actions. - Captures comprehensive history of changes in AWS accounts. - Helps you discover and troubleshoot security and operational issues.	**OPS 4**: How do you implement observability in your workload? **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? **OPS 7**: How do you know that you are ready to support a workload? **SEC 4**: How do you detect and investigate security events? **SEC 10**: How do you anticipate, respond to, and recover from incidents? **REL 12**: How do you test reliability?

Summary of requirements	AWS Considerations	Implementation
Apply encryption, integrity checks, and access controls for tamper-resistant logs with criticality-based retention periods, plus automated alerting for integrity failures or unauthorized access. **Align log management with regulatory requirements**, industry standards, and the AI's risk management framework.	- Supports tamper-proof log integrity validation. **Amazon CloudWatch Logs** - Centralizes logs from systems, applications, and AWS services. - Provides single, highly scalable service for log management. - Helps you search for specific error codes or patterns. - Supports filtering based on specific fields. - Allows secure archival for future analysis. - Presents logs as consistent flow of events ordered by time. **AWS Config** - Continually assesses, audits, and evaluates configurations and relationships of resources. - Works across AWS, on-premises, and other clouds. - Provides configuration history and change tracking. - Supports compliance auditing and security analysis. **Amazon GuardDuty** - Continuously monitors for malicious activity and unauthorized behavior. - Protects AWS accounts and workloads. - Provides intelligent threat detection. - Supports automated response to security events. **AWS Security Hub** - Provides comprehensive view of security alerts and compliance status. - Aggregates, organizes, and prioritizes security findings. - Helps you perform automated compliance checks. *Independent Validation and Assurance* **AWS Artifact** - Provides on-demand access to AWS security and compliance reports. - Includes SOC 1, SOC 2, SOC 3 reports. - ISO 27001, 27017, 27018 certifications. - PCI DSS compliance reports. - Helps you validate AWS-managed controls through independent third-party audits. **AWS Audit Manager** - Facilitates continuous auditing of AWS usage. - Automates evidence collection. - Helps assess risk and compliance with regulations and industry standards. *Encryption and Security* **AWS Key Management Service (AWS KMS)** - Manages encryption keys for log data. - Provides centralized control over cryptographic keys.	

Summary of requirements	AWS Considerations	Implementation
	- Integrates with CloudTrail and CloudWatch Logs for encrypted log storage. **AWS CloudHSM** - Hardware-based key storage for highly sensitive log encryption keys. - FIPS-validated HSMs for regulatory compliance. *Additional Considerations* **AWS Support Plans** – Available to provide personalized support for operational issues and technical questions (Basic, Developer, Business, Enterprise). **AWS Well-Architected Framework** – Provides consistent approach to evaluate architectures around six pillars including operational excellence and security. **AWS Enterprise Agreement** – Provides contractual framework designed for financial institutions	

Principle 8A: Workforce strategy and resource 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
AIs must maintain adequate in-house competencies across Board, senior management, and three lines of defence for effective cloud oversight and operations. Board and senior management need sufficient technical/managerial knowledge; operational teams require implementation expertise. Workforce planning must adapt to evolving cloud adoption. External expertise should strategically complement, not replace, internal accountability for critical cloud functions. **Define documented competency frameworks** and role-based training translating oversight expectations into skill requirements for Board, senior management, and three lines of defence staff. **Conduct regular skills-gap analyses** across business, technology, risk, legal, and compliance functions to identify current and emerging cloud competency needs. **Develop and review workforce plans reflecting cloud maturity,** operational demands, strategy, and risk appetite, including succession and knowledge retention measures. **Adjust workforce priorities as cloud adoption progresses**—specialist expertise for migrations, resilience/optimization focus for later stages. **Engage external expertise strategically with defined scopes**, competency checks, and knowledge transfer to maintain post-contract capability. **Avoid sustained external reliance for core functions; retain key responsibilities** (security oversight, critical workload monitoring, CSP	**Customer responsibility** - Competency Framework Development - Skills Gap Analysis and Workforce Planning - Strategic External Expertise Engagement - Adaptive Workforce Strategy *AWS services and resources that can help support this requirement:* *Training and Knowledge Development* **AWS Training and Certification** provides comprehensive training offerings including the following: - Role-based learning paths - Technical training courses - Business and executive training - Certification programs validating cloud expertise For more information, see AWS Training and Certification. *Architectural Guidance and Best Practices* **AWS Well-Architected Framework** helps cloud architects build secure, high-performing, resilient, and efficient infrastructure. The framework provides the following: - Consistent approach to evaluate architectures - Guidance across six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability - Best practices for implementing scalable designs *Documentation and Resources* **AWS Documentation** – Comprehensive technical documentation for all AWS services **AWS Whitepapers** – Industry-specific guidance and best practices **AWS Security Best Practices** – Guidelines for implementing security controls	**OPS 2**: How do you structure your organization to support your business outcomes? **OPS 3**: How does your organizational culture support your business outcomes? **OPS 1**: How do you determine what your priorities are? **COST 1**: How do you implement cloud financial management?

Summary of requirements	AWS Considerations	Implementation
evaluation) internally through periodic resource balance reviews.	**AWS Compliance Programs** – Documentation of AWS compliance with various standards and regulations *Support and Expert Guidance* **AWS Support Plans** provide four tiers of support with the following: - Access to technical support engineers - Architectural guidance - Operational support For more information, see AWS Support Plans. **AWS Professional Services** provides strategic engagement for complex implementations and migrations. **AWS Account Teams** provide dedicated support for enterprise customers. *Monitoring and Operational Tools* **AWS Health Dashboard** – Personalized view of service performance and availability **AWS Trusted Advisor** – Automated recommendations for optimization across multiple categories **AWS Security Hub** – Centralized security and compliance monitoring *Knowledge Transfer Support* **AWS Partner Network (APN)** – Access to validated partners for specialized expertise with structured engagement models **AWS Managed Services** – Optional managed services that can complement internal teams while maintaining customer control	

Principle 8B: Workforce training and competency development

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

Summary of requirements	AWS Considerations	Implementation
Establish structured, role-specific training programmes to ensure Board, senior management, and staff across three lines of defence maintain current knowledge and skills for effective cloud oversight and resilient operations. Training should be regular, address core cloud management dimensions, and be continually updated for latest technology, regulatory, and operational developments. **Programme design**: Create training with clear objectives, tailored curricula, and measurable outcomes covering governance, security, compliance, and operations for all relevant roles. **Timing and delivery**: Provide regular training, particularly before significant cloud adoption or migration events to prepare staff for new responsibilities. **Multi-platform proficiency**: Develop expertise across multiple CSP platforms, covering common and CSP-specific features, and maintain skills inventory tracking competency levels. **Needs assessment:** Regularly review training requirements with input from management, staff, and CSPs, reflecting evolving technologies, regulations, and business priorities. **Certification management**: Monitor professional certifications for alignment with cloud strategy and operational needs, track renewals, and encourage advanced certifications in emerging technologies. **Continuous improvement**: Use training evaluations, feedback, and incident lessons learned to enhance	**Customer responsibility** - Defining and implementing their own internal training and awareness programs for their workforce, including Board members, senior management, and staff across all three lines of defense. *AWS services and resources that can help support this requirement:* *Training and Certification Resources* **AWS Training and Certification** - Comprehensive training offerings covering various AWS services and cloud competencies - Role-based learning paths for different job functions - For more information, see AWS Training and Certification **AWS Skill Builder** - On-demand digital training platform - Hands-on labs and practice environments - Learning paths aligned to specific roles and certifications **AWS Certification Programs** - Industry-recognized certifications across multiple levels: - Foundational (Cloud Practitioner) - Associate (Solutions Architect, Developer, SysOps Administrator) - Professional (Solutions Architect, DevOps Engineer) - Specialty (Security, Advanced Networking, Machine Learning, and more) *Documentation and Knowledge Resources* **AWS Documentation** - Comprehensive technical documentation for all AWS services - Best practices guides and implementation patterns - For more information, see AWS Documentation **AWS Well-Architected Framework** - Guidance on building secure, high-performing, resilient, and efficient infrastructure	**OPS 3**: How does your organizational culture support your business outcomes? **OPS 2**: How do you structure your organization to support your business outcomes? **OPS 11**: How do you evolve operations? **SEC 11**: How do you incorporate and validate security properties of apps during design, development, and deployment lifecycle?

Summary of requirements	AWS Considerations	Implementation
programme content, delivery methods, and frequency. **External personnel**: Ensure CSPs and subcontractors receive training on security, incident response, and regulatory requirements; verify adequacy through training evidence review or contractual terms.	- Six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability - Provides consistent approach for evaluating architectures **AWS Whitepapers and Guides** - Industry-specific guidance (including financial services) - Security and compliance best practices - Architecture patterns and reference implementations *Compliance and Security Resources* **AWS Artifact** - On-demand access to AWS compliance reports and certifications - SOC reports, ISO certifications, PCI DSS reports - Helps staff understand AWS control environment **AWS Security Hub** - Centralized view of security and compliance status - Helps staff understand security posture and requirements **AWS Compliance Programs** - Information on AWS alignment with various regulatory frameworks - For more information, see AWS Compliance Programs *Support and Advisory Services* **AWS Support Plans** - Technical support from AWS engineers - Four tiers available (Basic, Developer, Business, Enterprise) - Enterprise Support includes Technical Account Manager (TAM) **AWS Professional Services** - Advisory and implementation support - Can assist with training needs assessment and program development **AWS Partner Network (APN)** - Access to AWS Partner training and certification programs - Training delivery partners for customized programs	

Document revisions

Date	Description
February 2026	First publication.