Guide to Financial Services Regulations in Argentina

B.C.R.A. Communications “A” 7,777 and 7,783

August 2024

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current 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.

Contents

Abstract

This document provides information to assist banks and financial services institutions in Argentina regulated by the Central Bank of Argentina (Banco Central de la República Argentina, or B.C.R.A.) as they adopt and accelerate their use of the Amazon Web Services (AWS) Cloud.

This guide describes the roles that AWS and customers play in managing and securing the cloud environment, describes the AWS Shared Responsibility Model, and provides an overview of the regulatory requirements from the B.C.R.A. that regulated financial institutions can consider when adopting AWS.

Introduction

The central bank of Argentina, the Banco Central de la República Argentina, or B.C.R.A. is the primary financial supervisory authority in Argentina responsible for the regulation, inspection, and supervision of financial institutions, including banking and credit institutions, and providers of payment services.

In June 2023, the B.C.R.A. issued Communication “A” 7,777 and Communication “A” 7,783, to update the general outsourcing guidelines (the B.C.R.A. Regulation) that financial institutions (FIs)[1] regulated by the B.C.R.A. must follow when outsourcing information technology (IT) services to a third-party technology provider, including the use of cloud services. All these updates are available in the texts *Minimum requirements for the management and control of technology and information security risks*[2] and *Minimum requirements for the management and control of technology and information security risks associated with digital financial services*[3], both applicable to banks, that is; *financial entities*[4]. In addition, the B.C.R.A. has published regulatory guidance through several public Normative Interpretations (or Interpretaciones Normativas) available on the B.C.R.A. website. These Normative Interpretations have clarified the scope of the B.C.R.A. Regulation with respect to financial institutions outsourcing to cloud service providers (CSPs).

The B.C.R.A. Regulation defines, among other things, the minimum technical and operational requirements that FIs should put in place for the management, implementation, and control of risks related to information technology, information systems, and other resources when outsourcing IT services to a third-party service provider, including the use of cloud services.

This guide is a resource to help financial institutions in Argentina understand the technical and operational requirements that may apply to them under the B.C.R.A. Regulation when they use AWS. This document also describes the AWS compliance framework and advanced tools and security measures which Financial Institutions may find helpful for evaluating and demonstrating their compliance with the applicable regulatory requirements under the B.C.R.A. Regulation.

A full analysis of the B.C.R.A. Regulation is beyond the scope of this guide. However, the sections outlined below address the primary considerations that recurrently arise in our interactions with financial institutions in Argentina and provide information that such institutions can use to help them understand their responsibilities and those of AWS under the B.C.R.A. regulation.

- **Security and shared responsibility:** financial institutions understand the AWS Shared Responsibility Model before evaluating the specific technical and operational requirements outlined in the B.C.R.A. Regulation. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS with respect to security and information access.
- **AWS Compliance programs:** AWS has obtained certifications and third-party attestations for a variety of industry-specific workloads. AWS has also developed compliance programs to make these resources available to customers. Customers can use the AWS compliance programs to help satisfy their regulatory requirements.
- **AWS Global Cloud Infrastructure:** The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones (AZs). The AWS Global Cloud Infrastructure offers AWS customers a more effective way to design and operate applications and databases, making them more available, fault tolerant, and scalable than traditional on-premises environments. AWS customers can use the AWS Global Cloud Infrastructure to help them design an AWS environment consistent with their business and regulatory needs, including applicable requirements under the B.C.R.A. Regulation.
- **Considerations on the B.C.R.A. Regulation:** This section describes common considerations for financial institutions that use AWS as they consider some of the key technical and operational requirements of the B.C.R.A. Regulation and describes how financial institutions can use AWS services and tools to help them comply with their regulatory requirements. A list of summarized requirements and corresponding considerations is provided in the Appendix, AWS considerations on operational and security requirements under the B.C.R.A. Regulation.

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

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 the B.C.R.A. Regulation. AWS manages 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 customer. Namely, customers retain control of the security programs that they choose to implement to protect their content, applications, systems, and networks. Customers assume responsibility and management of the guest operating system (including updates and security patches) and other associated application software in addition to the configuration of the AWS provided security group firewall.

Customers should 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 the flexibility and customer control that permits the deployment or workloads on AWS. Shown in the following chart, this differentiation of responsibility is referred to as security *of* the cloud versus security *in* the cloud.

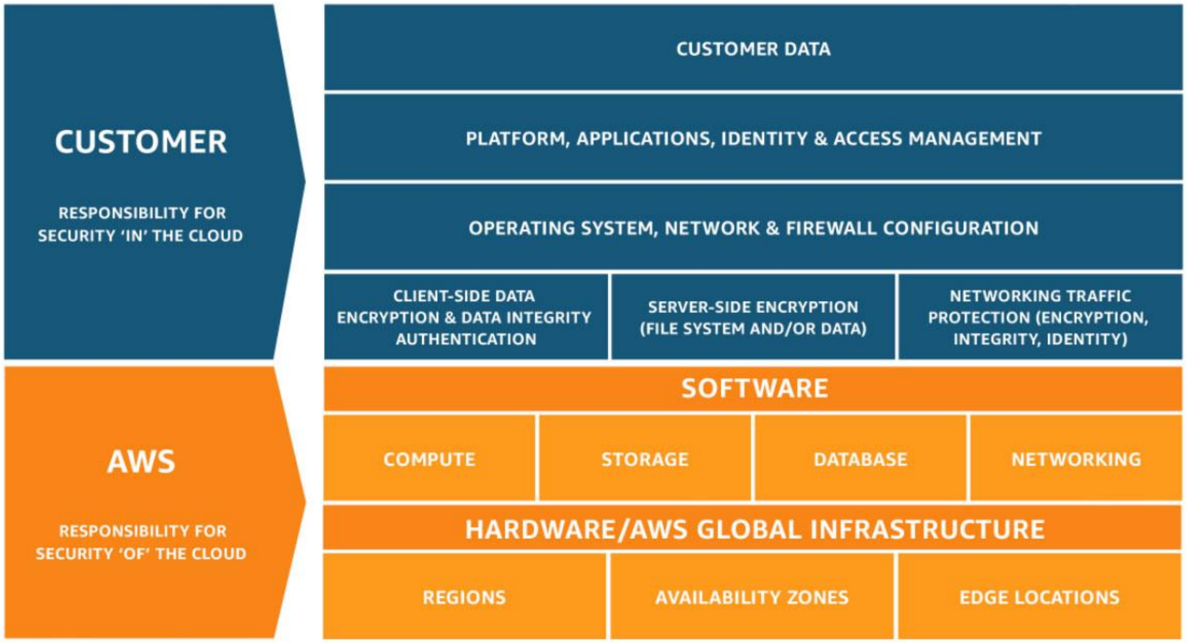
CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION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

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 of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

For abstracted 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.

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

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

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. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an information security management system that defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.
- **ISO 27017**: Provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional implementation guidance for information security controls specific to cloud service providers. For more information or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.
- **ISO 27018**: 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). It also provides a set of additional controls and associated guidance intended to address cloud PII protection requirements not addressed by the existing ISO 27002 control set. For more information or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.

- **ISO 27701** Specifies requirements and guidelines to establish and continuously improve the Privacy Information Management System (PIMS), including processing of Personally Identifiable Information (PII). It is an extension of the ISO/IEC 27001 and ISO/IEC 27002 standards for information security management providing a set of additional controls and associated guidance intended to address public cloud PIMS and PII management requirements for both processors and controllers, not addressed by the existing ISO/IEC 27002 control set. For more information, or to download the AWS ISO 27701 certification, see the ISO 27701 Compliance webpage.
- **ISO 22301**: Specifies the structure and requirements to implement, maintain, and improve a business continuity management system (BCMS) to protect against, reduce the likelihood of the occurrence of, prepare for, respond to, and recover from disruptions when they arise. Compliance to this standard provides assurance on AWS commitment to business continuity and resiliency of AWS services. For more information or to download the AWS ISO 22301 certification, see the ISO 22301 Compliance webpage.
- **ISO 9001**: Outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures that are required to achieve effective quality management within an organization. The key to the ongoing certification under this standard is establishing, maintaining, and improving the organizational structure, responsibilities, procedures, processes, and resources so AWS products and services consistently satisfy ISO 9001 quality requirements. For more information or to download the AWS ISO 9001 certification, see the ISO 9001 Compliance webpage.
- **PCI DSS Level 1**: The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD), including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. AWS is certified as a PCI DSS Level 1 Service Provider, the highest level of assessment available. For more information or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.

- **SOC**: AWS System and Organization Control (SOC) reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls that have been established to support operations and compliance. For more information, see the SOC Compliance webpage. AWS SOC reports come in three forms:
  - **SOC 1**: Provides information about the AWS control environment that might be relevant to a customer's internal controls over financial reporting, in addition to information for the assessment of the effectiveness of internal controls over financial reporting.
  - **SOC 2**: Provides customers and their service users that have a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
  - **SOC 3**: Provides customers and their service users that have a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality, without disclosing AWS internal information.

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

AWS Artifact

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

Support plans

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

Basic Support is included for all AWS customers and includes:

- Customer Service and Communities offer 24x7 access to customer service, documentation, whitepapers, and support forums.

- AWS Trusted Advisor is designed to provide seven core Trusted Advisor checks and guidance to provision resources following best practices to increase performance and improve security.
- AWS Personal Health Dashboard is designed to provide a personalized view of the health of AWS services, and alerts when customer resources are impacted.

AWS Global Cloud Infrastructure

The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones. A Region is a physical location in the world that consists of multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, all housed in separate facilities. These Availability Zones offer customers the ability to operate applications and databases, which are more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment. Customers can learn more about these topics by downloading our whitepaper Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

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

Considerations on the B.C.R.A Regulation

The focus of this guide is on Communication “A” 7,777 and Communication “A” 7,783 issued by the B.C.R.A. which regulate the outsourcing of services by financial institutions, including the use of cloud services.

Outsourcing by financial institutions

The B.C.R.A. Regulation allows financial institutions to outsource entirely or partially to a third-party service provider a broad set of information technology services, including the use of cloud services.

Section 10 of the consolidated text *Minimum requirements for the management and control of technology and information security risks* (amended by Communication “A” 7,777 and Communication “A” 7,783) and Section 1 of the consolidated text *Minimum requirements for the management and control of technology and information security risks associated with digital financial services*, known as *Disposiciones Generales*, introduced by Communication “A” 7,783, define general considerations that financial institutions should consider when outsourcing IT services to a third-party service provider, including:

- Prior notification requirement (see Notification section).
- The technical and operational requirements that financial institutions may need to implement depending on the nature and type of the outsourced activities.
- Notification requirements, including a list of information that financial institutions need to submit to the regulator.
- Responsibility: financial institutions that decide to outsource services remain nevertheless responsible to comply with applicable laws and regulations, and rules issued by the B.C.R.A.

Notification

Section 1 of the consolidated text *Minimum requirements for the management and control of technology and information security risks associated with digital financial services* (*Disposiciones Generales*, amended by Communication “A” 7,783) does not require financial entities to obtain a formal approval from the B.C.R.A. or the Superintendencia de Entidades Financieras y Cambiarias del Banco Central (SEFyC) prior to outsourcing IT services, but instead financial institutions are required to notify such outsourcing to the SEFyC at least 60 calendar days prior to the commencement of the outsourced activities, including the characteristics of the product or service, the protective measures adopted, the authentication factors used, planned monitoring activities, and activities for the management of cyber incidents, among others.

It should be noted that financial market infrastructures (FMIs) are required to notify such outsourcing to the SEFyC, but no prior time period is established for such notification. See Section 4.1.3. of the consolidated text *Minimum requirements for the management and control of technology and information security risks*.

Regulatory supervision, audit, and inspection

In June 2019, the B.C.R.A. published regulatory guidance in the form of Normative Interpretations to clarify the scope of the B.C.R.A. Regulation with respect to financial institutions outsourcing to cloud service providers. The Normative Interpretations acknowledge that the review of international, third-party certifications (such as the ISO certifications) and independent third-party audit reports (such as the SOC reports) are generally sufficient to satisfy the B.C.R.A. and the SEFyC audit and access rights with respect to cloud service providers providing services to financial institutions. This clarification highlights how these third-party certifications, attestations, and audit reports are valuable compliance resources that benefit the financial institutions and the regulators in their oversight of the outsourced activities. For more information about these third-party certifications and audit reports, see the AWS compliance programs section of this guide.

AWS customers have the option to enroll in an Enterprise Agreement with AWS. Enterprise agreements give customers the option to tailor agreements that best suit their needs, including any regulatory requirements.

Through an AWS Enterprise Agreement, AWS offers its customers regulated by the B.C.R.A. a contractual framework that helps them satisfy applicable contractual requirements under the B.C.R.A. Regulation, including specific terms that address a regulator’s access and inspection rights, where required by applicable law and under certain conditions. For more information about AWS Enterprise Agreements, contact your AWS representative.

Technical and operational requirements

The consolidated text *Minimum requirements for the management and control of technology and information security risks associated with digital financial services* (introduced by Communication “A” 7,783) defines minimum requirements for the management and control of technology and information security risks associated with digital financial services. Sections 2, 3, and 4 in the text outline a set of requirements applicable to financial services provided by digital media:

- Section 2: Risk management of financial services provided through digital means.
- Section 3: Protection of financial services provided by digital means.
- Section 4: Detection and monitoring.

Financial institutions should consider the workloads involved, the relevant categories of data and services to be outsourced, and assess the materiality or criticality of the relevant workloads in light of the requirements outlined in the B.C.R.A. Regulation and their operational risk management policies. As requirements differ by customer, AWS encourages each customer to obtain appropriate advice on their compliance with all regulatory and legal requirements that are relevant to their business, including the minimum technical and operational requirements included in the B.C.R.A. Regulation, and other local regulations and laws.

For further information on the technical and operational requirements described in the B.C.R.A. Regulation, see Appendix: AWS considerations on operational and security requirements under the B.C.R.A. Regulation.

Getting started

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

For financial institutions in Argentina, the next steps typically include the following:

- Contact your AWS representative to discuss how the AWS Partner Network (APN), and AWS Solutions Architects, Professional Services teams, and training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please contact us.
- Obtain and review a copy of the latest AWS SOC 1 and SOC 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 the cloud journey and use cases. These industry-accepted best practices, provide AWS customers with clear, step-by-step implementation and assessment recommendations.
- Explore other governance and risk management practices as necessary, do due diligence and risk assessment, by 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 customers maximize the use of the technology provided by AWS, the AWS technical team can support customers in their efforts to implement architecture, products, and services in compliance with applicable technical and operational requirements under the B.C.R.A. Regulation.

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 customer 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 possible for their applications. This framework is designed to provide a consistent approach for customers and AWS Partners to evaluate architectures, and provides guidance to help implement designs that scale application needs over time. The AWS Well-Architected Framework consists of six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability.
- AWS whitepapers on the six pillars of the AWS Well-Architected Framework: Operational Excellence Pillar; Security Pillar; Reliability Pillar; Performance Efficiency Pillar; Cost Optimization Pillar, and the Sustainability Pillar.
- Global Financial Services Regulatory Principles: AWS has identified five common principles related to financial services regulation that customers should consider when using AWS services and specifically, applying the Shared Responsibility Model to their regulatory requirements. You 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: AWS considerations on operational and security requirements under the B.C.R.A. Regulation

The following sections list key technical and operational requirements identified Sections 2, 3, and 4 of Communication “A” 7,783 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, security, reliability, performance efficiency, cost optimization, and sustainability—the AWS Well-Architected Framework is designed to provide a consistent approach for customers to evaluate architectures and implement designs that scale over time.

The table is organized into the following columns:

- **Summary of requirements:** Summarizes the requirements identified in the B.C.R.A. Regulation.
- **AWS Considerations:** Explains the considerations for addressing the requirements identified in the B.C.R.A. Regulation. 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 in the B.C.R.A. Regulation.
- **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.

Summary of requirements	AWS Considerations	Implementation
Section 2. Risk management of financial services provided by digital means. Financial institutions must apply principles and practices to identify, analyze, and mitigate the risks associated with the provision of financial services by digital means.		
Risk analysis shall consider at least:		
a) Operational risks, especially those related to internal and customer fraud, and those related to information technology and security.	**Customer Responsibility** AWS customers are responsible for defining their operational process model for managing systems, databases, and services, as well as the risk assessment process they use.	SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines? SEC 6. How do you protect your compute resources? REL 10. How do you use fault isolation to protect your workload?
b) The risks inherent in the mechanisms by which digital financial services are provided.	**Customer Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	OPS 5. How do you reduce defects, ease remediation, and improve flow into production? SEC 1. How do you securely operate your workload? SEC 6. How do you protect compute resources? OPS 8. How do you utilize workload observability in your organization?
c) The risks linked to opening customer accounts without the customer being present, customer authentication factors, and the authorization or confirmation of instructions made by customers in digital services.	**Shared Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use. Customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows customers to control user and programmatic access to AWS services and resources. AWS customers can apply granular policies, which assign permissions to a user, group, role, or resource. Customers also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). AWS customers can use federation with their existing directory service. For workloads that require systems to have access to AWS, AWS Identity and Access Management	SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines?

	(IAM) enables secure access through roles, instance profiles, identity federation, and temporary credentials.	
d) The impact on the organization's end-to-end risks.	**Customer Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	OPS 6. How do you mitigate deployment risks?
e) Scenarios that affect operational resilience.	**Shared Responsibility** AWS customers are responsible for properly implementing contingency planning, training, and testing for their systems hosted on AWS. AWS customers can utilize AWS to enable disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. AWS supports many popular Disaster Recovery (DR) architectures, from *pilot light* environments that are ready to scale up at a moment's notice to *hot standby* environments that enable rapid failover. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance backups, data redundancy replication, and the flexibility to place instances, and store data within multiple geographic Regions as well as across multiple Availability Zones within each Region. The AWS infrastructure has a high level of availability and is designed to provide customers the features they need to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. The AWS data centers are designed to anticipate and tolerate failure while maintaining service levels. In the case of failure, automated processes move customer data traffic away from the affected area. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable to architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve their recovery time and recovery point objectives, as well as the highest levels of service availability.	OPS 9. How do you understand the health of your operations? 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)?

	Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are typically physically separated within a metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by AWS Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, AWS Availability Zones are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are redundantly connected to multiple tier-1 transit providers. The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The AWS Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of nearly continuous improvement. AWS tests the Business Continuity Plan and its associated procedures at least annually to test effectiveness of the plan and the organization readiness. Customers can refer to the SOC 2 report in AWS Artifact for further information. Additionally, AWS has obtained ISO 22301:2019 certification. Alignment with ISO 22301 shows to customers that AWS has an effective Business Continuity Management System (BCMS) in place to support compliance with the global security and resiliency standard, ISO 22301:2019. The independent third-party assessment of this internationally recognized code of practice demonstrates the AWS commitment to the business continuity and resiliency of AWS services. Customers can learn more about these topics by downloading: Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond, and Disaster Recovery of Workloads on AWS: Recovery in the Cloud.	
Section 3. Protection of financial services provided by digital means.		
3.1. Guidelines to consider in digital financial transactions. Financial institutions must have duly identified and documented the digital services provided and the functionality of each of them. They must also design and implement controls for transactions aligned with the results of risk management and threat and vulnerability management. These controls will need to be adapted to transactional monitoring scenarios and they must cover, as a minimum:		
a) The customer must be identified and authenticated in order to carry out any type of transaction	**Customer Responsibility**	SEC 2. How do you manage authentication for people and machines?

b) Implement multi-factor authentication techniques according to the levels of risk, the results of transactional monitoring and when they exceed established risk thresholds.	AWS customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows customers to control user and programmatic access to AWS services and resources. AWS customers can apply granular policies, which assign permissions to a user, group, role, or resource and also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). Customers can also use federation with their existing directory service. For workloads that require systems to have access to AWS, AWS Identity and Access Management (IAM) enables secure access through roles, instance profiles, identity federation, and temporary credentials. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected from disclosure. AWS provides an advanced set of access, encryption, and logging features such as AWS CloudTrail to help financial institutions do this effectively. AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. Changes to customer environments can be detected and tracked using AWS Services such as AWS Config to assess, audit, and evaluate the configurations of AWS resources. AWS customers can configure logging throughout the workload, including application logs, resource logs, and AWS service logs. For example, ensure that AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub are enabled for all accounts within their organization. AWS customers can use automation to investigate and remediate events to reduce human effort and error, which can enable them to scale investigation capabilities. Regular reviews help tune automation tools, and iterate. For example, AWS customers can automate responses to events by automating the first investigation step, then iterate to gradually remove human effort with Amazon GuardDuty, a security monitoring	SEC 3. How do you manage permissions for people and machines? SEC 5. How do you protect network resources? SEC 6. How do you protect compute resources? OPS 8. How do you utilize workload observability in your organization? REL 6. How do you monitor workload resources? These best practices cover secure authentication, access control, network and compute resource protection, performance monitoring, and resource monitoring, which are essential for implementing customer identification, authentication, and risk-based multi-factor authentication in digital financial services on AWS.

	service that helps identify unexpected and potentially unauthorized or unexpected activity in the customer's AWS environment. In addition, the AWS Personal Health Dashboard gives AWS customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and is designed to provide proactive notification to help AWS customers plan for scheduled activities.	
3.1.1. Confirmation of critical actions. Apply multi-factor authentication or digital identification techniques, in the confirmation or authorization for the execution of at least the following critical actions:		
a) Creating, enabling, and rehabilitating authentication factors. **b)** Subscribing to new products or services, applying for pre-approved credits, or accepting new terms of use. **c)** Changes to contact information or operational parameters related to a transaction. **d)** Schedule a third-party account for transfers. **e)** Confirmation of transactions that deviate from predetermined patterns in transactional monitoring systems.	**Customer Responsibility** AWS customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows customers to control user and programmatic access to AWS services and resources. AWS customers can apply granular policies, which assign permissions to a user, group, role, or resource and also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). Customers can also use federation with their existing directory service. For workloads that require systems to have access to AWS, AWS Identity and Access Management (IAM) enables secure access through roles, instance profiles, identity federation, and temporary credentials. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected from disclosure. AWS provides an advanced set of access, encryption, and logging features such as AWS CloudTrail to help financial institutions do this effectively. AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. Changes to customer environments can be detected and tracked using AWS Services such as AWS Config to assess, audit, and evaluate the configurations of AWS resources.	SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines?

	AWS customers can configure logging throughout the workload, including application logs, resource logs, and AWS service logs. For example, ensure that AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub are enabled for all accounts within their organization. AWS customers can use automation to investigate and remediate events to reduce human effort and error, which can enable them to scale investigation capabilities. Regular reviews help tune automation tools, and iterate. For example, AWS customers can automate responses to events by automating the first investigation step, then iterate to gradually remove human effort with Amazon GuardDuty, a security monitoring service that helps identify unexpected and potentially unauthorized or unexpected activity in the customer's AWS environment. In addition, the AWS Personal Health Dashboard gives AWS customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and is designed to provide proactive notification to help AWS customers plan for scheduled activities.	
3.1.2. Confirmation of non-critical actions.		
For low-risk actions, use randomized pre-configured customer questions, or a non-predictable, single-use secure code.	**Customer Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines?
3.1.3. Services based on telephone service or messaging platforms. When, in order to operate accounts, customers use the telephone or a messaging platform, financial institutions must:		
a) Enable the functionality according to the results of risk analysis and the strength of authentication factors. **b)** Implement a real-time log of all information related to the transactions. **c)** Avoid exposure of authentication factors **d)** Immediate refund to customer if a transaction carried out in this way is not recognized by the customer.	**Customer Responsibility** AWS customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows customers to control user and programmatic access to AWS services and resources. AWS customers can apply granular policies, which assign permissions to a user, group, role, or resource and also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). Customers can also use federation with their existing directory service.	SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines? SEC 5. How do you protect network resources? SEC 6. How do you protect compute resources? OPS 8. How do you utilize workload observability in your organization? REL 6. How do you monitor workload resources?

	For workloads that require systems to have access to AWS, AWS Identity and Access Management (IAM) enables secure access through roles, instance profiles, identity federation, and temporary credentials. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected from disclosure. AWS provides an advanced set of access, encryption, and logging features such as AWS CloudTrail to help financial institutions do this effectively. AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. Changes to customer environments can be detected and tracked using AWS Services such as AWS Config to assess, audit, and evaluate the configurations of AWS resources. AWS customers can configure logging throughout the workload, including application logs, resource logs, and AWS service logs. For example, ensure that AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub are enabled for all accounts within their organization. AWS customers can use automation to investigate and remediate events to reduce human effort and error, which can enable them to scale investigation capabilities. Regular reviews help tune automation tools, and iterate. For example, AWS customers can automate responses to events by automating the first investigation step, then iterate to gradually remove human effort with Amazon GuardDuty, a security monitoring service that helps identify unexpected and potentially unauthorized or unexpected activity in the customer's AWS environment. In addition, the AWS Personal Health Dashboard gives AWS customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and is designed to provide proactive notification to help AWS customers plan for scheduled activities.	
3.2. Devices and applications provided by the organization.		

Financial institutions must design and implement security measures for devices and applications provided to customers using digital financial services according to the results of risk management and threat and vulnerability management. The devices and applications include ATMs, self-service terminals and digital kiosks, mobile banking, internet banking, and digital wallets.	**Shared Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use. Customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring, and intrusion detection for their instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services, listed on AWS Customer Support Policy for Penetration Testing. AWS utilizes a wide variety of automated monitoring systems designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity and alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. Responses are performed according to incident response processes and procedures. AWS takes security very seriously, and investigates all reported vulnerabilities. AWS customers can report vulnerabilities and security concerns regarding AWS services or open source projects by submitting a Vulnerability Report. AWS is committed to being responsive and keeping AWS customers informed of our progress as we investigate and mitigate reported security concerns. AWS customers receive a non-automated response to their initial contact within 24 hours, confirming receipt of the reported vulnerability. AWS customers receive progress updates from AWS at least every five U.S. working days. AWS Security performs regular vulnerability scans on the underlying infrastructure, web application, and databases in the AWS environment using a variety of tools. External vulnerability assessments are conducted by an AWS approved third-party vendor at least quarterly, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. AWS customers can validate the AWS controls using the SOC 2 report available through AWS Artifact.	SEC 5. How do you protect network resources? SEC 6. How do you protect compute resources? REL 5. How do you design interactions in a distributed system to mitigate or withstand failures?

	AWS operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Security teams subscribe to newsfeeds for applicable vendor flaws and proactively monitor the websites of vendors and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield is designed to provide always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield: Standard and Advanced. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against common, frequently occurring network and transport layer DDoS attacks that target websites or applications. When AWS customers use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, they receive comprehensive availability protection against known infrastructure (Layer 3 and 4) attacks. AWS customers can use AWS Shield Advanced for higher levels of protection against attacks. In addition to the network and transport layer protections that come with AWS Shield Standard, AWS Shield Advanced is designed to provide additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall. AWS WAF is a web application firewall that helps protect web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. AWS WAF gives control over how traffic reaches applications by enabling the creation of security rules that control bot traffic and block common attack patterns, such as SQL injection or cross-site scripting.	
Financial institutions shall consider information security aspects throughout the lifecycle of devices and applications provided to customers. They must apply controls such as:	**Shared Responsibility** Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they	SEC 8. How do you protect data at rest? SEC 9. How do you protect data in transit? SEC 10. How do you anticipate, respond to, and recover from incidents?

a) Data exchanged must remain encrypted throughout the interaction with the customer. **b)** Implement measures to detect and terminate unauthorized client sessions. **c)** Disable the service and prevent the entry of customer authentication factors when failures occur that can compromise the security of the service. **d)** When the customer is redirected to third-party sites enabling banking transactions, the customer's authentication factors should not be shared with those third parties.	use them. AWS customers can encrypt their content, and we provide customers with the option to manage their own encryption keys. AWS customers choose how their content is secured. AWS offers encryption features to protect content in transit and at rest. AWS provides customers with options to manage their own encryption keys. These data protection features include: • Data encryption capabilities available in over 100 AWS services. • Flexible key management options using AWS Key Management Service (AWS KMS), allowing customers to choose whether to have AWS manage their encryption keys or enabling customers to keep complete control over their keys. AWS protects the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help ensure that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected. AWS provides several methods for customers to securely handle their data. AWS customers can use AWS CloudHSM service for creating and managing cloud-based hardware security modules. A hardware security module (HSM) is a specialized security device that generates and stores cryptographic keys. If AWS customers need to secure their encryption keys in a service backed by FIPS-validated HSMs, but do not need to manage the HSM, they may consider AWS Key Management Service (AWS KMS). For the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage. For more information, visit S3 User Guide Protecting Data Using Server-Side Encryption. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring, and intrusion detection for their instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services, listed on AWS Customer Support Policy for Penetration Testing. AWS utilizes a wide variety of automated monitoring systems designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network	OPS 8. How do you utilize workload observability in your organization? OPS 10. How do you manage workload and operations events?

	usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity and alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. Responses are performed according to incident response processes and procedures. AWS takes security very seriously, and investigates all reported vulnerabilities. AWS customers can report vulnerabilities and security concerns regarding AWS services or open source projects by submitting a Vulnerability Report. AWS is committed to being responsive and keeping AWS customers informed of our progress as we investigate and mitigate reported security concerns. AWS customers receive a non-automated response to their initial contact within 24 hours, confirming receipt of the reported vulnerability and receive progress updates from AWS at least every five U.S. working days. AWS Security performs regular vulnerability scans on the underlying infrastructure, web application, and databases in the AWS environment using a variety of tools. External vulnerability assessments are conducted by an AWS approved third-party vendor at least quarterly, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. AWS customers can validate AWS controls using the SOC 2 report available through AWS Artifact. AWS operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Security teams subscribe to newsfeeds for applicable vendor flaws and proactively monitor the websites of vendors and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield is designed to provide always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield: Standard and Advanced.	

	All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against common, frequently occurring network and transport layer DDoS attacks that target websites or applications. When AWS customers use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, they receive comprehensive availability protection against known infrastructure (Layer 3 and 4) attacks. AWS customers can use AWS Shield Advanced for higher levels of protection against attacks. In addition to the network and transport layer protections that come with AWS Shield Standard, AWS Shield Advanced is designed to provide additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall. AWS WAF is a web application firewall that helps protect web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. AWS WAF gives control over how traffic reaches applications by enabling the creation of security rules that control bot traffic and block common attack patterns, such as SQL injection or cross-site scripting.	
3.2.1 Applications provided by the financial institution. When deploying applications in customer-controlled environments, the financial institution must establish at least the following controls:		
a) Use installation methods that limit the exposure of personal, financial, or customer authentication data.	**Shared Responsibility** Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS offers customers the ability to add a layer of security to their data at rest in the cloud, providing scalable and efficient encryption features. These include: • Data at rest encryption capabilities available in AWS services, such as Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda, and Amazon SageMaker. • Flexible key management options, including AWS Key Management Service (AWS KMS), that allow AWS customers to choose whether to have AWS manage the encryption keys or keep complete control over their own keys. • Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing AWS customers to help satisfy their	SEC 8. How do you protect data at rest? SEC 9. How do you protect data in transit?

	compliance requirements. - Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS. In addition, AWS provides APIs to integrate encryption and data protection with the services developed or deployed in an AWS environment. For further information refer to Encrypting Data-at-Rest and -in-Transit, Data Encryption, and How to protect data in transit?. AWS protects the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help ensure that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected. AWS provides several methods for customers to securely handle their data. AWS customers can use AWS CloudHSM. AWS CloudHSM is a service for creating and managing cloud-based hardware security modules. A hardware security module (HSM) is a specialized security device that generates and stores cryptographic keys. If AWS customers need to secure their encryption keys in a service backed by FIPS-validated HSMs, but do not need to manage the HSM, they may consider AWS Key Management Service (AWS KMS). For the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage. For more information, visit S3 User Guide Protecting Data Using Server-Side Encryption.	
b) Inform the client of the eligibility criteria of the client's devices, as well as the hardware, software, connectivity, and environment limitations for their use. Must also inform the security requirements applicable to the customer's own devices. **c)** Prevent access through a device that does not meet the identified eligibility criteria. **d)** Implement measures that mitigate risks associated with operating system configurations of mobile devices. **e)** Only request the minimum permissions required to operate the application.	**Customer Responsibility** AWS customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows customers to control user and programmatic access to AWS services and resources. AWS customers can apply granular policies, which assign permissions to a user, group, role, or resource and also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). Customers can also use federation with their existing directory service.	SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines? SEC 5. How do you protect network resources? SEC 6. How do you protect compute resources? REL 6. How do you monitor workload resources?

f) Associate the application with the mobile device and with the customer, at time of registration or in a subsequent re-installation. **g)** Validate that the device in use is the one associated by the customer and implement controls to handle SIM card changes. **h)** Provide mechanisms for blocking access to the application and automatic blocking of the session due to inactivity ("time out").	For workloads that require systems to have access to AWS, AWS Identity and Access Management (IAM) enables secure access through roles, instance profiles, identity federation, and temporary credentials. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected from disclosure. AWS provides an advanced set of access, encryption, and logging features such as AWS CloudTrail to help financial institutions do this effectively. AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. Changes to customer environments can be detected and tracked using AWS Services such as AWS Config to assess, audit, and evaluate the configurations of AWS resources. AWS customers can configure logging throughout the workload, including application logs, resource logs, and AWS service logs. For example, ensure that AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub are enabled for all accounts within their organization. AWS customers can use automation to investigate and remediate events to reduce human effort and error, which can enable them to scale investigation capabilities. Regular reviews help tune automation tools, and iterate. For example, AWS customers can automate responses to events by automating the first investigation step, then iterate to gradually remove human effort with Amazon GuardDuty, a security monitoring service that helps identify unexpected and potentially unauthorized or unexpected activity in the customer's AWS environment. In addition, the AWS Personal Health Dashboard gives AWS customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and is designed to provide proactive notification to help AWS customers plan for scheduled activities.	
3.2.2. Devices provided by the financial institution.		
Devices will need to be identified and authenticated to operate.	**Customer Responsibility**	SEC 2. How do you manage authentication for people and machines?

Approval processes for devices that allow interaction with the customer must include formal verification and approval prior to their enablement. When devices use physical or virtual keyboards, authentication factors must be encrypted immediately upon entry. In addition, authentication data shall not be stored on the device provided by the organization or retained in the activity log.	AWS customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows customers to control user and programmatic access to AWS services and resources. AWS customers can apply granular policies, which assign permissions to a user, group, role, or resource and also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). Customers can also use federation with their existing directory service. For workloads that require systems to have access to AWS, AWS Identity and Access Management (IAM) enables secure access through roles, instance profiles, identity federation, and temporary credentials. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected from disclosure. AWS provides an advanced set of access, encryption, and logging features such as AWS CloudTrail to help financial institutions do this effectively. AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. Changes to customer environments can be detected and tracked using AWS Services such as AWS Config to assess, audit, and evaluate the configurations of AWS resources. AWS customers can configure logging throughout the workload, including application logs, resource logs, and AWS service logs. For example, ensure that AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub are enabled for all accounts within their organization. AWS customers can use automation to investigate and remediate events to reduce human effort and error, which can enable them to scale investigation capabilities. Regular reviews help tune automation tools, and iterate. For example, AWS customers can automate responses to events by automating the first investigation step, then iterate to gradually remove human effort with Amazon GuardDuty, a security monitoring	SEC 3. How do you manage permissions for people and machines? SEC 5. How do you protect network resources? SEC 6. How do you protect compute resources? REL 6. How do you monitor workload resources?

	service that helps identify unexpected and potentially unauthorized or unexpected activity in the customer's AWS environment. In addition, the AWS Personal Health Dashboard gives AWS customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and is designed to provide proactive notification to help AWS customers plan for scheduled activities.	
3.2.2.1. Protection of audit logs. Implement measures to protect audit trails, both digital and on paper. The controls applied shall be in accordance with the results of the risk analysis and shall assess at least:		
a) Storage conditions, **b)** Mechanisms for log transmission or transport.	**Customer Responsibility** AWS customers designate in which geographic region their content will be located. With AWS, financial institutions can determine where their content will be stored, including the type of storage and geographic region of that storage. They can replicate and back up their content in more than one Region, and AWS will not move or replicate customer data outside of the Region the customer chooses, except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users. For current information on AWS Regions and Availability Zones, see Global Infrastructure. AWS customers choose the secured state of their content. We offer financial institutions strong encryption for content in transit or at rest, and we provide them with the option to manage their own encryption keys. AWS customers manage access to their content and AWS services and resources through users, groups, permissions and credentials that they control.	SEC 8. How do you protect data at rest? SEC 9. How do you protect data in transit?
c) Methods for safe destruction of media. **d)** Access control measures.	**Shared Responsibility** Customers are responsible for managing the entire lifecycle of the devices they own. AWS maintains a systematic approach to planning and developing new services for the AWS environment to help meet quality and security requirements with each release. The strategy that AWS employs for the design and development of services is to clearly define services in terms of customer use cases, service performance, marketing and distribution requirements, production and testing, and legal and regulatory requirements. The design of new services or any significant changes to current services follow secure	OPS 6. How do you mitigate deployment risks? SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines?

	software development practices and are controlled through a project management system with multi-disciplinary participation. Requirements and service specifications are established during service development, taking into account legal and regulatory requirements, customer contractual commitments, and requirements to meet the confidentiality, integrity and availability of the service. Service reviews are completed as part of the development process. AWS tracks, documents, and verifies media sanitization and disposal actions. Media removal and disposal is performed by designated AWS personnel. AWS hosts are securely wiped or overwritten prior to provisioning for reuse. AWS media is securely wiped or degaussed and physically destroyed prior to leaving AWS Secure Zones. Media storage devices used to store customer data are classified by AWS as *critical* and treated accordingly, as high impact, throughout their lifecycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned. To validate the secure wipe processes and procedures in use by AWS, third-party auditors review the guidance within the AWS Media Protection policy, observe degaussing equipment and secure shred bins located within AWS facilities, and observe historical tickets tracking the destruction of a hard drive within a data center and the process of a device being wiped and removed from the environment. **Data deletion for block device-based storage (Amazon EBS, Amazon RDS, ephemeral drives):** AWS wipes underlying storage media upon re-provisioning rather than upon de-provisioning. Processes that wipe content upon release of an asset (volume, object) are less reliable than processes that re-provision clean storage to customers. Physical servers can reboot at any time for many reasons (power outage, system process interruption or failure), which might leave a wiping procedure in an incomplete state. Customers do not have access to block devices or physical media that was previously used to store another customer's content. For example, in the case of Amazon EBS, customers see their content or zeros (empty disk) after writing a block or partial block. Wiping blocks at the time that	

	storage capacity is re-provisioned prevents recovering previous content from a new volume or object. **Data deletion for non-block device services:** For services such as Amazon S3 or DynamoDB, customers do not see an attached block device, but objects and the path to that object (a table or an item). When a customer deletes an asset in these services, the deletion of the mapping between an asset identifier or key and the underlying content begins immediately. Once the mapping is removed, the content is no longer accessible and cannot be processed by an application. In AWS, privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows customers to control user and programmatic access to AWS services and resources. AWS customers using IAM can apply granular policies which assign permissions to a user, group, role, or resource. Customers also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). AWS customers can use federation with their existing directory service. For workloads that require systems to have access to AWS, IAM enables secure access through roles, instance profiles, identity federation, and temporary credentials. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected from disclosure. AWS provides an advanced set of access, encryption, and logging features such as AWS CloudTrail to help financial institutions do this effectively. AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users.	
3.2.2.2. Physical controls on devices provided. Devices should incorporate features that reduce the risk of copying, obstruction, third-party viewing, or illegal retention of authentication factors and monetary values, considering, but not limited to, the application of the following controls:		
a) Detect unauthorized objects attached to devices provided by the organization. **b)** Add anti-skimming measures to the input of authentication factors.	**Customer Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	Not applicable.

c) Mechanisms for detecting the unauthorized disassembly of the device, or the alteration of the physical and/or logical properties of the device.		
3.2.2.3. Controls on the maintenance and configuration of provided devices. The processes of maintaining and configuring devices provided by the organization shall:		
a) Implement a physical and logical segregation between administrative activities (installation and configuration of the operating system or application) and the regular operation of the device. **b)** Apply controls to the opening and closing of the device and the use and possession of physical and/or logic keys. **c)** Provide supporting documentation and record operational activities.	**Customer Responsibility** AWS customers define their governance and operational model, as well as the risk assessment process they use. AWS customers maintain ownership of their content, and select which AWS services can process, store, and host their content. AWS customers can choose the AWS Regions in which their content will be located and can choose to deploy their AWS services exclusively in a single Region if preferred. Customers can define the architecture of their workloads to meet specific geographic or regulatory requirements and can work with their AWS account manager and their AWS architect for assistance on architecture definition. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected. AWS customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. The AWS compliance programs help customers understand the robust controls in place at AWS to maintain security and compliance in the cloud. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS compliance programs help customers to establish and operate in an AWS security control environment. The IT standards that AWS complies with are broken out by Certifications and Attestations; Laws, Regulations and Privacy; and Alignments and Frameworks. Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. AWS customers remain responsible for complying with applicable compliance laws, regulations and privacy programs. The AWS compliance programs include, but are not limited to AWS Service Organization Control (SOC) 1, 2, and 3 reports, ISO 27001, ISO 27017,	SEC 1. How do you securely operate your workload? SEC 5. How do you protect network resources? SEC 6. How do you protect compute resources? SEC 7. How do you classify your data? SEC 8. How do you protect data at rest? SEC 9. How do you protect data in transit?

	ISO 22301, and ISO 27018 certifications, and PCI DSS compliance reports. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2, and 3 reports, ISO 27001, 27017 and 27018 certifications, and PCI DSS compliance reports. Reports and certifications can be downloaded using AWS Artifact. Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. AWS customers maintain full control over who has access to their data. Those services designed to provide virtualized operational environments to customers (Amazon EC2, for example) allow customers to be segregated from one another and prevent cross-tenant privilege escalation and information disclosure via hypervisors and instance isolation. Different instances running on the same physical machine are isolated from each other via the hypervisor. In addition, the Amazon EC2 firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. Packets must pass through this layer, and the neighbors to an Amazon EC2 instance have no more access to that instance than any other host on the Internet and they can be treated as if they are on separate physical hosts. The physical random-access memory (RAM) is separated using similar mechanisms. Customer instances have no access to physical disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically erases blocks of storage before making them available for use, which protects one customer's data from being unintentionally exposed to another. AWS customers can further protect their data using traditional filesystem encryption mechanisms, or, in the case of Amazon Elastic Block Store (EBS) volumes, by enabling AWS-managed disk encryption. Changes to customer environments can be detected and tracked using AWS Services such as AWS Config to assess, audit, and evaluate the configurations of AWS resources. AWS customers can configure logging throughout their workloads, including application logs, resource logs, and AWS service logs. For example, ensure that AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub are enabled for all accounts within their organization.	

AWS customers can use automation to investigate and remediate events to reduce human effort and error, which can enable them to scale investigation capabilities. Regular reviews help tune automation tools, and iterate. For example, AWS customers can automate responses to events by automating the first investigation step, then iterate to gradually remove human effort with Amazon GuardDuty, a security monitoring service that helps identify unexpected and potentially unauthorized or unexpected activity in the customer's AWS environment.

In addition, the AWS Personal Health Dashboard gives AWS customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and is designed to provide proactive notification to help customers plan for scheduled activities.

AWS offers customers the ability to add a layer of security to their data at rest in the cloud, providing scalable and efficient encryption features. These include:

- Data at rest encryption capabilities available in AWS services, such as Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda, and Amazon SageMaker.
- Flexible key management options, including AWS Key Management Service (AWS KMS), that allow AWS customers to choose whether to have AWS manage the encryption keys or enable complete control over the customer's own keys.
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, helping AWS customers satisfy compliance requirements.
- Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS.

In addition, AWS provides APIs to integrate encryption and data protection with the services developed or deployed in an AWS environment. For further information refer to Encrypting Data-at-Rest and -in-Transit, Data Encryption, and How to protect data in transit?.

AWS protects the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help ensure that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected.

	AWS provides several methods for customers to securely handle their data. AWS customers can use AWS CloudHSM service for creating and managing cloud-based hardware security modules. A hardware security module (HSM) is a specialized security device that generates and stores cryptographic keys. If AWS customers need to secure their encryption keys in a service backed by FIPS-validated HSMs, but do not need to manage the HSM, they may consider AWS Key Management Service (AWS KMS). For the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage. For more information, visit S3 User Guide Protecting Data Using Server-Side Encryption.	
3.2.2.4. Proof of transaction.		
The devices must provide the customer with the possibility to print or send a receipt of the transaction to a pre-defined point of contact.	**Customer Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	Not applicable.
3.3. Digital identification of customers. If the financial institution allows digital and remote identification of customers, they must design processes that allow verification of the data provided to identify the customer. During the customer identification process, controls should:		
a) Validate the presence of the person and obtain proof of life. **b)** Validate the customer's contact information and the mobile device associated with the customer. **c)** Validate biometric elements and documentation submitted. Complementary techniques should be used to verify the identity of the financial service customer in the digital registration process in accordance with the results of the risk analysis.	**Customer Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines?
3.3.1. Registration process not completed. In the event that the registration process is not completed, the following controls must be applied to the data collected during the process:		
a) Do not disclose the reason(s) for the errors or failures in the identification process. **b)** Collected data must be deleted through a secure deletion process.	**Customer Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	SEC 8. How do you protect data at rest? SEC 9. How do you protect data in transit?

c) Data stored for statistical purposes must be anonymized.		
3.4. Access control. Requirements for authentication factors. Access identifiers used in digital financial services may not include personal or public customer data and options must be available to allow their modification. Establish these minimum measures to protect the authentication factors of digital financial services customers throughout their lifecycle:		
a) Authentication factors are not known by the staff of the financial institution or third parties, **b)** Authentication factors are stored only for verification, with measures to safeguard their confidentiality. **c)** Authentication factors are protected with cryptographic techniques. The authentication factors shall take into account the provisions set out in section 5.7.2. In addition, the following special provisions shall apply.	**Shared Responsibility** Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS customers can encrypt their content, and we provide customers with the option to manage their own encryption keys. AWS customers choose how their content is secured. AWS offers encryption features to protect customers' content in transit and at rest. AWS provides customers options to manage their own encryption keys. These data protection features include: • Data encryption capabilities available in over 100 AWS services. • Flexible key management options using AWS Key Management Service (AWS KMS), allowing customers to choose whether to have AWS manage their encryption keys or enabling customers to keep complete control over their keys. AWS protects the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help ensure that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected. AWS provides several methods for customers to securely handle their data. AWS Customers can use AWS CloudHSM service for creating and managing cloud-based hardware security modules. A hardware security module (HSM) is a specialized security device that generates and stores cryptographic keys. If AWS customers need to secure their encryption keys in a service backed by FIPS-validated HSMs, but do not need to manage the HSM, they may consider AWS Key Management Service (AWS KMS). For the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage. For more information, visit S3 User Guide Protecting Data Using Server-Side Encryption.	SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines? SEC 8. How do you protect data at rest? SEC 9. How do you protect data in transit?
3.4.1. Memorized Secret:		

Authenticators based on memorized secrets (or something you "know") must meet the following controls:		
a) Minimum length of eight characters. **b)** Include lowercase and uppercase letters, numbers, and special characters. **c)** Must be changed on the first use. **d)** Limit exposure when customer enters them to authenticate. **e)** Limit the speed of entry through automated access (for example, Captcha). **f)** Limit unsuccessful login attempts according to risk analysis. **g)** When secrets are created or modified, detailed information must be provided to customers on the minimum requirements for the secret and the reasons for rejection.	**Customer Responsibility** AWS customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows customers to control user and programmatic access to AWS services and resources. AWS customers can apply granular policies, which assign permissions to a user, group, role, or resource and also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). Customers can also use federation with their existing directory service. For workloads that require systems to have access to AWS, AWS Identity and Access Management (IAM) enables secure access through roles, instance profiles, identity federation, and temporary credentials. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected from disclosure. AWS provides an advanced set of access, encryption, and logging features such as AWS CloudTrail to help financial institutions do this effectively. AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. Changes to customer environments can be detected and tracked using AWS Services such as AWS Config to assess, audit, and evaluate the configurations of AWS resources. AWS customers can configure logging throughout the workload, including application logs, resource logs, and AWS service logs. For example, ensure that AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub are enabled for all accounts within their organization. AWS customers can use automation to investigate and remediate events to reduce human effort and error, which can enable them to scale investigation capabilities. Regular reviews help tune automation tools,	SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines?

	and iterate. For example, AWS customers can automate responses to events by automating the first investigation step, then iterate to gradually remove human effort with Amazon GuardDuty, a security monitoring service that helps identify unexpected and potentially unauthorized or unexpected activity in the customer's AWS environment. In addition, the AWS Personal Health Dashboard gives AWS customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and is designed to provide proactive notification to help AWS customers plan for scheduled activities.	
3.4.2. Out-of-band authentication. Out-of-band authenticators shall comply with the following controls:		
a) Not visible when the device is locked. **b)** Comply with requirements for one-time passkeys (OTPs). **c)** Only registered devices can read cryptogram graphics.	**Customer Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	Not applicable.
3.4.3. One-time passkeys (OTP). When using one-time passkeys (OTP)-based authenticators, implement the following controls:		
a) Control of the device where the OTP is displayed. **b)** Generated value valid for less than 120 seconds. **c)** Minimum length of 6 digits. **d)** Define a seed length that ensures the generation of unique values. **e)** Encrypt channel and transmitted information.	**Shared Responsibility** Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS offers customers the ability to add a layer of security to their data at rest in the cloud, providing scalable and efficient encryption features. These include: • Data at rest encryption capabilities available in AWS services, such as Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda, and Amazon SageMaker. • Flexible key management options, including AWS Key Management Service (AWS KMS), that allow AWS customers to choose whether to have AWS manage the encryption keys or keep complete control over their own keys. • Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing customers to help satisfy their compliance requirements.	SEC 8. How do you protect data at rest? SEC 9. How do you protect data in transit?

	- Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS. In addition, AWS provides APIs to integrate encryption and data protection with the services developed or deployed in an AWS environment. For further information refer to Encrypting Data-at-Rest and -in-Transit, Data Encryption, and How to protect data in transit?. AWS protects the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help ensure that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected. AWS provides several methods for customers to securely handle their data. AWS customers can use AWS CloudHSM. AWS CloudHSM is a service for creating and managing cloud-based hardware security modules. A hardware security module (HSM) is a specialized security device that generates and stores cryptographic keys. If AWS customers need to secure their encryption keys in a service backed by FIPS-validated HSMs, but do not need to manage the HSM, they may consider AWS Key Management Service (AWS KMS). For the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage. For more information, visit S3 User Guide Protecting Data Using Server-Side Encryption.	
3.4.4. Payment cards (debit, credit, or prepaid), physical authentication elements, and secret personal identification number (PIN).		
3.4.4.1. Replacement of Provided Authentication Factors. **3.4.4.2.** Authentication factors withheld or not delivered to the customer. **3.4.4.3.** Authentication factors based on integrated circuit (chip) cards. **3.4.4.4.** Authentication factors based on magnetic stripe cards.	**Customer Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	Not applicable.
3.5. Training and awareness-raising. Financial institutions are required to develop specific training and awareness plans for digital financial services that include at least:		
a) Information about points of contact provided by the financial institution and guidelines for customers to verify them.	**Shared Responsibility** AWS Customers are responsible for defining their own internal Training and Awareness program. AWS customers can leverage AWS training	Not applicable.

b) Information about contact channels used to notify customers of situations that could compromise their security. In particular, how to identify the official accounts of the financial institution in social networks. **c)** Information referring to the configurable or parameterizable aspects that the customer has available in the digital financial service. **d)** Recommendations on the secure use and configuration of the customer's digital devices used for digital financial services. **e)** Information about social engineering techniques and security measures to protect against such techniques. **f)** Recommendations on the safe use of devices or applications provided by the financial services institution to customers. **g)** Information on the procedures that customers should follow to dispute a transaction, how to file a complaint, how to act in the event of suspected fraud, or in a situation of ongoing fraud, among others. Plans will need to be updated based on changes in the products and services made available to customers. For the plan updates, the results of transactional monitoring, new attack techniques and cyber incident management should also be considered.	services and resources to help their staff have the appropriate training and resources to manage AWS services. Training offerings are available at Training and Certification. AWS has implemented formal, documented security awareness, and training policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes. The policy is disseminated through the internal communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties. AWS has developed, documented and disseminated role-based security awareness training for employees responsible for designing, developing, implementing, operating, maintaining, and monitoring the systems managing security and availability and provides resources necessary for employees to fulfill their responsibilities.	
3.6. Means of communication. Financial institutions must offer communication channels—including alternative communication mechanisms—to their financial service customers for queries and complaints, and notification of cyber incidents or suspicious situations. Communication channels should be documented, use pre-validated customer touchpoints, and report events:		
a) Registration, deregistration, linking, or rehabilitation of authentication factors. **b)** Modification of personal data or transaction parameters. **c)** Transactional information. **d)** Financial institutions must make available to customers information on: - Date and time of last access to the service. - Authentication factors about to expire.	**Customer Responsibility** AWS customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	Not applicable.

- Records of transactions made, available in digital format for at least 90 days.		
4.1. Event detection and analysis.		
Financial institutions must establish a process for the registration and analysis of information related to security events in the systems, networks, and technological infrastructure that supports digital financial services, In addition, all systems and applications that support digital financial services must generate audit trails to ensure the traceability of each of the actions carried out.	**Shared Responsibility** Customers are responsible for defining their operational model based on the AWS services they choose to use. As part of the shared security responsibility model, security events monitoring should be performed by both AWS and AWS customers. AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub, and AWS Config Rules to track, monitor, analyze, and audit events. If these tools identify an event that is analyzed and determined to be an incident, that *qualifying event* raises an incident and triggers the incident management process and the appropriate response actions necessary to mitigate the incident. AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS utilizes a three-phased approach to manage incidents: 1. Activation and Notification Phase 2. Recovery Phase 3. Reconstitution Phase To test the effectiveness of the AWS Incident Management plan, AWS conducts incident response testing. This testing is designed to provide coverage for the discovery of previously unknown defects and failure modes. In addition, it allows the AWS Security and AWS service teams to test for potential customer impact and further prepare staff to handle incidents such as detection and analysis, containment, eradication, and recovery, and post-incident activities. The plan is tested annually. AWS Incident Management planning, testing, and test results are reviewed by third party auditors. Customers can access this information through the SOC 2 report available in AWS Artifact. Customers can learn more about this topic by downloading: AWS Security Incident Response Guide and NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud.	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?

	In addition, the AWS Personal Health Dashboard gives customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and is designed to provide proactive notification to help customers plan for scheduled activities.	
4.2. Monitoring of customer activity and transactions. Financial institutions must define a monitoring strategy to detect unusual activity or suspicious customer transactions in digital financial services. The transactional monitoring solutions must consider the results of the risk analysis, behavior patterns, and the authentication factors used. In addition, they must apply the following criteria to their monitoring strategy:		
a) Classify transaction initiators and beneficiaries to determine thresholds, activity patterns, and alerts. **b)** Monitor transaction frequency by type, transaction amount, and regular account balances. **c)** Compromised authentication factors, known fraud patterns, indications of malware on the devices used. **d)** Patterns of customer behavior in the use of the device or application. **e)** Identification of common points of compromise that may affect customer transactions. Additionally, transactional monitoring of the authentication factors provided to customers should facilitate detection of compromise of sensitive data. Financial institutions should define action models based on the results of the risk analysis, the behavior patterns and the usual circumstances of the use of the application and the authentication factors. The models will be able to combine preventive, reactive and assumed measures: • **Preventive**: communicate with the customer through side channels before confirming transactions. • **Reactive**: communicate with the customer after suspicious transactions are found.	**Customer Responsibility** AWS customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows customers to control user and programmatic access to AWS services and resources. AWS customers can apply granular policies, which assign permissions to a user, group, role, or resource and also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). Customers can also use federation with their existing directory service. For workloads that require systems to have access to AWS, AWS Identity and Access Management (IAM) enables secure access through roles, instance profiles, identity federation, and temporary credentials. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected from disclosure. AWS provides an advanced set of access, encryption, and logging features such as AWS CloudTrail to help financial institutions do this effectively. AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. Changes to customer environments can be detected and tracked using AWS Services such as AWS Config to assess, audit, and evaluate the configurations of AWS resources.	SEC 2. How do you manage authentication for people and machines? SEC 3. How do you manage permissions for people and machines? SEC 5. How do you protect network resources? SEC 6. How do you protect compute resources? OPS 9. How do you understand the health of your operations? REL 6. How do you monitor workload resources?

• **Assumed**: make customers whole when they dispute transactions. Financial institutions are required to apply a process of continuous improvement to their transactional monitoring solutions, action models and incident management, in accordance with the evolution of emerging fraudulent techniques, and information on fraud trends collected from internal or external sources. They shall monitor the use and evolution of social engineering techniques aimed at the financial institution, its customers, and the third parties involved in the services. Financial institutions need to take preventive and timely actions to remove fake accounts and applications, fake websites, and malicious content. Detection and monitoring processes shall be integrated with cyber incident management.	AWS customers can configure logging throughout the workload, including application logs, resource logs, and AWS service logs. For example, ensure that AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub are enabled for all accounts within their organization. AWS customers can use automation to investigate and remediate events to reduce human effort and error, which can enable them to scale investigation capabilities. Regular reviews help tune automation tools, and iterate. For example, AWS customers can automate responses to events by automating the first investigation step, then iterate to gradually remove human effort with Amazon GuardDuty, a security monitoring service that helps identify unexpected and potentially unauthorized or unexpected activity in the customer's AWS environment. In addition, the AWS Personal Health Dashboard gives AWS customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and is designed to provide proactive notification to help AWS customers plan for scheduled activities.	

Document revisions

Date	Description
June 2024	Initial draft.
August 2024	First publication.

[1] Financial institutions include banks, Payment Service Providers (PSP) and Financial Market Infrastructures (FMIs).

[2] See the B.C.R.A. consolidated text *Minimum requirements for the management and control of technology and information security risks* (applicable to banks and FMIs) in the following link: https://www.bcra.gob.ar/Pdfs/Texord/t-rmgcti.pdf

[3] See the B.C.R.A. consolidated text *Minimum requirements for the management and control of technology and information security risks associated with digital financial services* (applicable to banks and PSPs, but not FMIs) in this link: https://www.bcra.gob.ar/Pdfs/Texord/t-rmrtsd.pdf

[4] Financial entities are those institutions subject to the framework established in Law No. 21,526 (that is, banks). Financial entities are included under the umbrella concept of financial institutions.