aws FOR FINANCIAL SERVICES

AWS User Guide to the Digital Operational Resilience Act (DORA)

June 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 regarding the adoption of Amazon Web Services (AWS) cloud for entities who are subject to the forthcoming Digital Operational Resilience Act (DORA).

This guide describes the roles that AWS and its customers play in managing operational resilience in and on AWS, describes the AWS Shared Responsibility Model, compliance frameworks, advanced tools, and security measures that customers can use to evaluate their compliance with applicable regulatory requirements; with an overview of the DORA regulatory requirements and guidance that regulated customers can consider when adopting AWS.

Introduction

The Digital Operational Resilience Act (DORA) is a pan-European legislative framework on operational resilience and cyber resilience. DORA outlines improvements in information and communications technology (ICT) and security risk-management requirements, a harmonization regime for ICT incident reporting, development of a digital operational resilience testing framework, and an oversight framework for critical ICT third-party providers. DORA does not set any restrictions or limitations on financial entities (FEs) subject to DORA requirements for their adoption and use of cloud services.

DORA sets uniform requirements for FEs to achieve a high common level of digital operational resilience. It covers requirements related to ICT risk management, reporting of major ICT-related incidents and cyber threats, digital operational resilience testing, information sharing on cyber threats and vulnerabilities, and measures for managing ICT third-party risk. The regulation promotes a principles-based approach to ICT risk management, giving FEs the flexibility to use different management models as long as they address key functions such as: identification, protection, detection, response, recovery, and communications. DORA requires FEs to maintain updated and resilient ICT systems that can handle stressed market conditions and adverse situations, and mandates efficient business continuity and recovery plans to limit damage and ensure prompt resumption of activities after ICT-related incidents.

This user guide provides a series of considerations on how FEs seeking to meet the regulatory expectations set by DORA can utilize AWS services and documentation to help demonstrate their compliance with DORA requirements.

Operational Resilience and the AWS Shared Responsibility Model

AWS and the financial services industry share a common interest in maintaining operational resilience capabilities, such as the ability to provide continuous service despite disruptions. Continuity of services, especially for critical functions, is a key prerequisite for financial stability and AWS recognizes that financial institutions using AWS services need to comply with sector-specific regulatory obligations and internal requirements regarding operational resilience including, but not limited to, DORA.

At AWS, we define operational resilience as the ability to provide continuous service through people, processes, and technology that are aware of, and adaptable to, constant change. It is a real-time, execution-oriented norm embedded in the culture of AWS that is distinct from traditional approaches in information security, business continuity, disaster recovery, and crisis management; that rely primarily on centralized, hierarchical programs focused on documentation development and maintenance.

However, operational resilience is a shared responsibility; AWS is responsible for ensuring that the services used by AWS customers—the building blocks of their applications—are continuously available, and ensuring that AWS is prepared to handle a wide range of events that could affect our cloud infrastructure. AWS customers are responsible for designing, testing, and deploying their applications on AWS in a manner that achieves the availability and resiliency they need, including those mission-critical applications that require that AWS services are available when customers need them; even upon the occurrence of a service impairment or disruption.

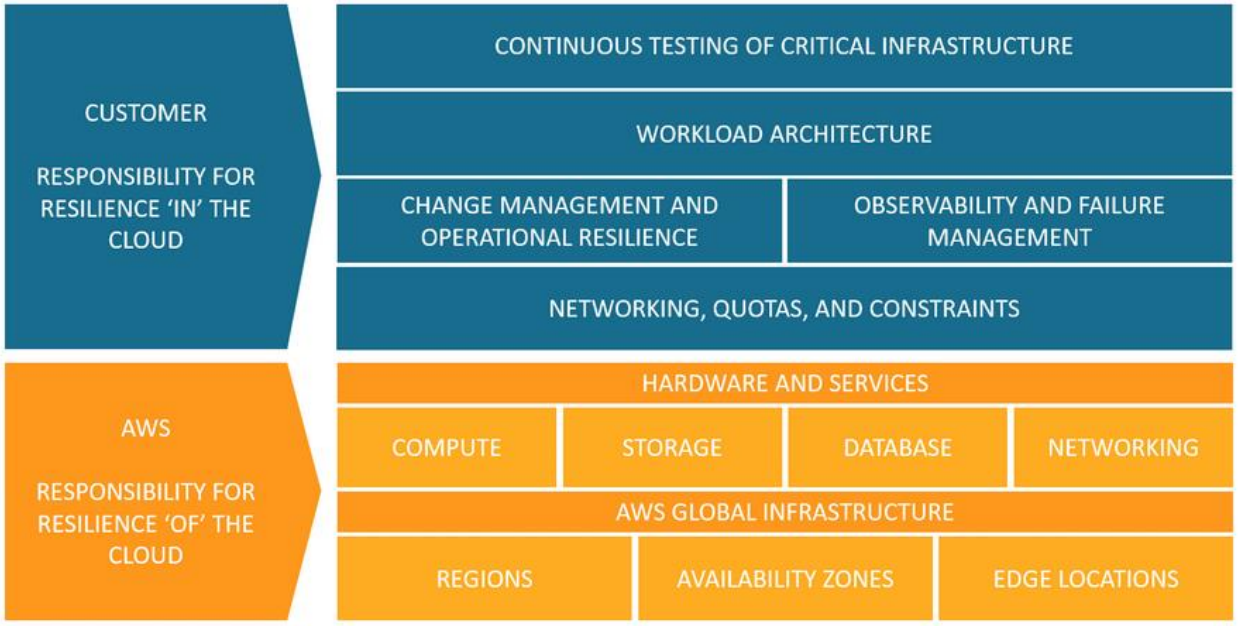

Figure 1 – The AWS Shared Responsibility Model for operational resilience

The AWS Shared Responsibility Model is fundamental to understanding the respective roles of AWS and its customers within the context of cloud services. AWS is responsible for the resiliency of the hardware, software, networking, and facilities that runs all of the services offered by AWS.

The responsibility of AWS customers will be determined by the AWS services they select, because the service selection determines the amount of configuration work that customers must perform as part of their resiliency responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) requires customers to perform all of the necessary resiliency configuration and management tasks. Customers that deploy EC2 instances are responsible for deploying EC2 instances across multiple locations (such as AWS Availability Zones), and can implement self-healing architectures using services such as Amazon EC2 Auto Scaling, as well as using resilient workload architecture best practices for applications installed on the EC2 instances.

For abstracted services, such as 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 resiliency of their data, including backup, versioning and replication strategies, classifying their assets, and using identity and access management (IAM) tools to apply the appropriate permissions.

Resilience in the Cloud

AWS customers are responsible for their resilience in the cloud and assume responsibility and management of the guest operating system (including updates and security patches) and other associated application software, as well as applicable network security controls. 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.

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 AWS 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.

AWS provides tools and information to assist customers assessing controls in their extended IT environment. For more information, refer to the AWS Compliance Center, Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond, AWS Shared Responsibility Model for Resiliency, and the AWS Well Architected Framework. Please contact your AWS representative to discuss how the AWS FSI Compliance team, the AWS Partner Network, as well as AWS Solution Architects, and Professional Services teams can assist.

Resilience of the Cloud

AWS infrastructure and services operate under several compliance standards and industry certifications across geographies and industries. Customers can use the AWS compliance certifications to validate the implementation and effectiveness of internal controls at AWS, including security best practices and certifications.

The AWS compliance program is based on the following actions:

Validating that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS

control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that customers can implement, and to better assist customers with managing their control environment.

Demonstrating the AWS compliance posture to help customers assess compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with information regarding the policies, processes, and controls that have been established and operated by AWS. FEs can use this information to perform their control evaluation and verification procedures.

Monitoring through security controls that allow AWS to demonstrate ongoing compliance with global standards and best practices.

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 FEs:

- **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 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, as well as 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.
- **C5:** Is an attestation supported by the German government and introduced in Germany by the Federal Office for Information Security (BSI). C5 helps organizations demonstrate operational security against common cyber-attacks when using cloud services within the context of the Security Recommendations for Cloud Providers issued by the German government. For more information, see the C5 Compliance webpage.

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

AWS Artifact

Customers can use AWS Artifact to review and download reports and details about more than 2,600 security controls. In addition, the AWS Artifact portal provides on-demand access to AWS security and compliance

documents, including SOC reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals.

AWS Global Cloud Infrastructure

The AWS Global Cloud Infrastructure comprises 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. FEs can learn more about these topics by downloading our whitepaper on Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond.

FEs choose the Region in which their content and servers are located. This allows FEs to establish environments that meet specific geographic or regulatory requirements. Additionally, FEs with business continuity and disaster recovery objectives can establish primary and backup environments in a location or locations of their choice. The majority of AWS customers can meet their business continuity and disaster recovery objectives within a single Region. More information on our disaster recovery recommendations is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

FEs operating in Europe have the choice to adopt and use any Region including eight separate Regions in Europe: Ireland, London, Frankfurt, Paris, Stockholm, Milan, Zurich, and Spain.

For example, if the FE chooses to deploy exclusively in the Spain Region, their content will be located in Spain unless the FE chooses to move that content. AWS will not move or replicate content outside of the chosen Region except as agreed with the FE.

All Regions are designed, built, and validated against rigorous compliance standards, providing high levels of security for FEs. All Regions are validated against applicable national and global data protection laws.

Due Diligence and Monitoring

AWS provides information about its control environment to customers through technical papers, reports, certifications, and third-party attestations. The AWS documentation helps customers understand the controls AWS has in place that are relevant to the AWS services customers use, and how those controls have been validated. This information can help FEs assess controls in their extended IT environment.

Traditionally, internal and external auditors validate the design and operational effectiveness of controls by process walkthroughs and evidence evaluation, but this type of direct observation and verification is generally performed in traditional on-premises deployments. Instead, FEs using AWS services can request and evaluate third-party attestations and certifications issued for AWS, in order to service their due diligence requirements.

Third-party attestations and certifications of AWS help customers review the design and operating effectiveness of control objectives and provide visibility and independent validation of the control environment by a qualified, independent third party. As a result, although some controls are managed by AWS, the control environment can be a unified framework where FEs can assess controls, accelerating the compliance review process.

The table that follows, presents the most common due diligence topics we identified in interactions with FEs and the AWS considerations to each item.

Due diligence topic	AWS considerations
Financial	The financial statements of Amazon.com Inc. include sales and income for AWS, permitting assessment of its financial position and ability to service its debts and/or liabilities. These financial statements are available from the United States Securities and Exchange Commission ("SEC") or via Amazon's Investor Relations website.
Technical capabilities, operational capability and capacity	Since 2006, AWS has provided flexible, scalable and secure IT infrastructure to businesses of all sizes around the world. AWS continues to grow and scale, allowing us to provide new services that help millions of active customers. The AWS Cloud operates a global infrastructure with multiple Availability Zones within multiple Regions around the world. For more information, see AWS Global Infrastructure. AWS performs a continuous risk assessment process to identify, evaluate, and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. The AWS risk management team monitors and escalates risks on a continuous basis, performing risk assessments on newly implemented controls at least every six months.
Monitor the third-party service provider's performance and compliance with its contractual obligations	AWS offers service level agreements for certain AWS services. These may be updated from time to time. The AWS Health Dashboard provides ongoing visibility into resource performance and the availability of AWS services and accounts. It displays relevant and timely information to help FEs manage events in progress, and provides proactive notification to help customers plan for scheduled activities. 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. For more information about AWS Enterprise Agreements, contact your AWS representative.

Due diligence topic	AWS considerations
Compliance with applicable laws and regulatory requirements in its jurisdiction	AWS has worked with some of the most complex financial services organizations at every stage of their respective cloud journeys and understands the importance of maintaining positive relationships with financial services regulators. AWS Artifact allows FEs to access and download AWS audit artifacts in order to share artifacts with regulators as evidence from AWS of security and compliance controls.
Outsourcing on a cross-border basis	AWS customers choose the Region in which their content and servers are located. This allows customers to establish environments that meet specific geographic requirements. Regions are designed, built, and validated against rigorous compliance standards, providing high levels of security for FEs. All Regions are validated against applicable national and global data protection laws.

Alignment to DORA for Cloud Services

FEs should consider assessing their workloads against AWS best practices as recommended within the AWS Well-Architected Framework. The AWS Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability—the AWS Well-Architected Framework provides a consistent approach for FEs to evaluate architectures and implement designs that scale over time.

FEs should also consider using the following AWS services to facilitate operational risk management activities: AWS Audit Manager, AWS Security Hub, AWS Resilience Hub, AWS Config and AWS Trusted Advisor.

FEs can use the independent assurance reports made available through AWS Artifact. AWS Artifact contains third-party attestations and certifications of AWS controls and environments that provide visibility and independent validation of the control environment by a qualified, independent third party. In particular, the SOC 2 and C5 reports provide relevant information for consideration by FEs.

In particular, AWS recommends FEs to inform their management of operational resilience using the following AWS prescriptive guidance:

- Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond
- AWS - Designing Highly Resilient Financial Services Applications
- AWS Prescriptive Guidance – Backup and Recovery approaches
- Disaster Recovery of Workloads on AWS: Recovery in the Cloud

The following tables can help FEs map expectations from key principles listed in the DORA regulation to relevant AWS resources. The tables are organized into the following columns:

Requirements references DORA requirements, sometimes in summary form. Always refer to the authoritative source text of DORA for verification.

AWS considerations on customer responsibilities when addressing DORA requirements, refers to the security and compliance of the cloud, or the AWS services that FEs can use to address these requirements.

Resources lists additional documentation that FEs may use to supplement the information in this guide

A full analysis of the all sections in DORA is beyond the scope of this user guide. The information that follows includes considerations that AWS specialists frequently encounter in interactions with FEs.

Requirements	AWS considerations on Customer Responsibilities	Resources
ICT Risk Management **Articles 4.1,4.2,4.3, 6**	AWS recommends FEs oversee and manage ICT risk within their cloud deployments in line with applicable standards and guidance. For assurance over their cloud deployments, FEs should consider assessing with AWS best practices as recommended within the AWS Well-Architected Framework. The AWS Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability—the AWS Well-Architected Framework provides a consistent approach for FEs to evaluate architectures and implement designs that scale over time. AWS also has a financial services industry lens for the Well-Architected Framework that FEs should consider. FEs should also consider using the following AWS services to facilitate risk management activities: AWS Audit Manager, AWS Security Hub, AWS Resilience Hub, AWS Config and AWS Trusted Advisor. FEs should also consult AWS guidance within Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond . For assurance over AWS global infrastructure, FEs should rely on the independent assurance made available through AWS Artifact. AWS recommends AWS Enterprise Support for FEs planning to operate mission-critical workloads on AWS. AWS Enterprise Support will assist FEs to manage, monitor, analyze and report on usage of AWS. AWS Enterprise Support provides FEs with proactive planning, architectural reviews, and consultative guidance including: strategic business reviews, security improvement programs, guided Well-Architected reviews, and cost optimization workshops. AWS Enterprise Support also provides FEs a response time within 15 minutes in the case of business-critical system going down.	AWS Well-Architected Framework AWS Well-Architected Framework - Financial Services Industry Lens Getting started with AWS Artifact AWS Audit Manager User Guide AWS Security Hub User Guide AWS Resilience Hub User Guide AWS Trusted Advisor User Guide AWS Config Developer Guide Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond . AWS Enterprise Support

Requirements	AWS considerations on Customer Responsibilities	Resources
Governance, control frameworks and roles and responsibilities Articles 5.1, 5.2	AWS recommends FEs consult the AWS Cloud Adoption Framework (AWS CAF) to inform the design and operation of their governance and control frameworks. The AWS CAF applies AWS experience and best practices to help FEs digitally transform and accelerate business outcomes through innovative use of AWS. AWS CAF identifies specific organizational capabilities that underpin successful cloud transformations. These capabilities provide best practice guidance that can help FEs improve cloud readiness. AWS CAF groups its capabilities in six perspectives: Business, People, Governance, Platform, Security, and Operations. The AWS CAF Governance perspective focuses on orchestration of cloud initiatives while maximizing organizational benefits and minimizing risks related to the digital transformation. AWS recommends FEs consult AWS prescriptive guidance on building a cloud operating model to inform FEs in the setting of clear roles and responsibilities and effective and timely communication, cooperation and coordination. AWS recommends AWS Enterprise Support for FEs planning to operate mission-critical workloads on AWS. AWS Enterprise Support will assist FEs to manage, monitor, analyze and report on usage of AWS. AWS Enterprise Support provides FEs with proactive planning, architectural reviews, and consultative guidance including: strategic business reviews, security improvement programs, guided Well-Architected reviews, and cost optimization workshops. AWS Enterprise Support also provides FEs a response time within 15 minutes in the case of business-critical system going down.	AWS Cloud Adoption Framework AWS CAF Governance perspective AWS Prescriptive Guidance - Building your Cloud Operating Model AWS Enterprise Support
Business Continuity Planning, ICT Response Planning and Digital Operational Resilience Testing	AWS recommends FEs consult the following guidance to inform their business continuity planning and ICT response planning: • Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond • AWS - Designing Highly Resilient Financial Services Applications • AWS Prescriptive Guidance – Backup and Recovery approaches • Disaster Recovery of Workloads on AWS: Recovery in the Cloud	AWS Well-Architected Framework Disaster Recovery of Workloads on AWS: Recovery in the Cloud AWS Resilience Hub User Guide AWS Fault Injection Service User Guide Amazon CloudWatch User Guide

Requirements	AWS considerations on Customer Responsibilities	Resources
Articles 5.2(e), 11, 12, 14, 24	For assurance over their cloud deployments, FEs should consider assessing with AWS best practices as recommended within the AWS Well-Architected Framework. The AWS Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability—the AWS Well-Architected Framework provides a consistent approach for FEs to evaluate architectures and implement designs that scale over time. FEs should also consider using the following AWS services to optimize resiliency: AWS Resilience Hub, AWS Fault Injection Service, Amazon CloudWatch, Amazon Route 53 Application Recovery Controller, AWS Elastic Disaster Recovery, AWS Backup and AWS Trusted Advisor. AWS recommends FEs consider engaging the AWS Customer Incident Response Team (CIRT) as required. AWS also recommends FEs regularly complete AWS Game Days to validate and optimize their operational resilience. For the resilience of the cloud, the AWS Resiliency Program encompasses the processes and procedures by which AWS identifies, responds to, and recovers from a major availability event or incident within the AWS services environment. This program builds upon the traditional approach of addressing contingency management that incorporates elements of business continuity and disaster recovery plans, and expands it to consider critical elements of proactive risk mitigation strategies, such as engineering physically separate Availability Zones (AZs) and continuous infrastructure capacity planning. AWS contingency plans and incident response playbooks are maintained and updated to reflect emerging risks and lessons learned from past incidents. Service team response plans are tested and updated through the due course of business, and the AWS Resiliency Plan is tested, reviewed, and approved by senior leadership annually.	Amazon Route53 Application Recovery Controller Developer Guide AWS Elastic Disaster Recovery User Guide AWS Backup Developer Guide AWS Trusted Advisor User Guide Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond . AWS - Designing Highly Resilient Financial Services Applications AWS Prescriptive Guidance – Backup and Recovery approaches AWS Well Architected Framework – Game Days
ICT Internal Audits Article 5.2(f)	AWS recommends FEs consider use of AWS Audit Manager, AWS Cloud Audit Academy, AWS Artifact and the AWS Compliance portal to support ICT audit plans and audits. AWS Audit Manager helps continually audit AWS usage to help manage risk and compliance with regulations and industry standards. Audit Manager automates evidence collection so FEs can assess whether policies, procedures, and activities—also known as controls—are operating effectively.	AWS Artifact AWS Audit Manager User Guide AWS Cloud Audit Academy AWS Compliance

Requirements	AWS considerations on Customer Responsibilities	Resources
	The AWS Cloud Audit Academy is a Security Auditing Learning Path designed for existing and prospective auditing, risk, and compliance professionals who are involved in assessing regulated workloads in the cloud. For assurance of the cloud, AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. Internal and external audits are planned and performed according to a documented audit schedule to review the continued performance of AWS against standards-based criteria, like the ISO/IEC 27001 and to identify improvement opportunities. Compliance reports from these assessments are made available to customers, enabling them to evaluate AWS. FEs can access assessments from AWS Artifact. The AWS compliance reports identify the scope of AWS services and regions assessed, as well as the assessor's attestation of compliance. FEs can perform vendor or supplier evaluations by leveraging these reports and certifications.	
Information Security Management Articles 13, 19, 25	AWS recommends FEs consult the following guidance to inform their information security management: • Introduction to AWS Security • AWS Cloud security - Shared Responsibility Model • Security Pillar - AWS Well-Architected Framework • AWS Best Practices for DDoS Resiliency • AWS Security Reference Architecture (SRA) • AWS Security Incident Response Guide • Navigating GDPR Compliance on AWS AWS recommends FEs consider use of the following key security services within their AWS environment: • AWS Identity and Access Management (IAM) • AWS Organizations • AWS Control Tower • Amazon GuardDuty	Introduction to AWS Security AWS Cloud security - Shared Responsibility Model Security Pillar - AWS Well-Architected Framework AWS Best Practices for DDoS Resiliency AWS Security Reference Architecture (SRA) AWS Security Incident Response Guide Navigating GDPR Compliance on AWS AWS Identity and Access Management (IAM) AWS Organizations AWS Control Tower

Requirements	AWS considerations on Customer Responsibilities	Resources
	• AWS Security Hub • AWS Config • AWS Shield and Shield Advanced • Amazon CloudWatch • AWS CloudTrail • AWS Key Management Service (AWS KMS) • Amazon Inspector • AWS Artifact • AWS Audit Manager To optimize the security of cloud deployments, FEs should consider assessing with AWS best practices as recommended in the AWS Well-Architected Framework Security Pillar. For security of the cloud, AWS has an established information security organization that is managed by the AWS Security team and is led by the AWS Chief Information Security Officer (CISO). The responsibilities of the AWS Security team are defined and allocated across the organization. The AWS Security team works with AWS service teams, other internal security teams, and external parties to mitigate security risks. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access, privacy, and security. AWS also has established an information security framework and regularly reviews and updates the security policies, provides security training—which includes data classification—to employees, and performs application security reviews. These reviews assess the availability, confidentiality, and integrity of data, as well as conformance to the security policies. Where necessary, AWS Security leverages the security framework and security policies established and maintained by Amazon Corporate Information Security.	Amazon GuardDuty Amazon Inspector AWS Security Hub AWS Config AWS Shield and Shield Advanced Amazon CloudWatch AWS CloudTrail AWS Key Management Service (AWS KMS) AWS Artifact AWS Audit Manager
Key Contractual Provisions Article 30	The current AWS EBA, EIOPA & ESMA Financial Services Addendum contains terms and conditions that help FEs address existing financial services regulatory requirements, such as those present under the EBA, EIOPA, and ESMA Guidelines. AWS will make updated terms available for customers, as required, once final DORA provisions are clear. Many subsidiary portions of DORA are yet to be finalized.	AWS Enterprise Agreements AWS Enterprise Support

Requirements	AWS considerations on Customer Responsibilities	Resources
	AWS recommends AWS Enterprise Support for FEs planning to operate mission-critical workloads on AWS. AWS Enterprise Support will assist FEs to manage, monitor, analyze and report on usage of AWS. AWS Enterprise Support provides FEs with proactive planning, architectural reviews, and consultative guidance including: strategic business reviews, security improvement programs, guided Well-Architected reviews, and cost optimization workshops. AWS Enterprise Support also provides FEs a response time within 15 minutes in the case of business-critical system going down.	

Next Steps

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

For FEs, the next steps typically include the following:

- Evaluate cloud deployments ("in the cloud") against the AWS Well-Architected Framework and the Financial Services Industry Lens to build secure, high-performing, resilient, and efficient infrastructure.

- Consult AWS guidance such as:
  - Introduction to AWS Security
  - AWS Security and Compliance - Shared Responsibility Model
  - AWS Shared Responsibility Model for Resiliency
  - AWS Well-Architected Framework - Security Pillar
  - AWS Well-Architected Framework - Reliability Pillar
  - Disaster Recovery of Workloads on AWS: Recovery in the Cloud
  - AWS - Designing Highly Resilient Financial Services Applications
  - Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond

- Review the use of AWS services against existing or planned cloud workloads

  Resilience of cloud workloads

  - AWS Resilience Hub
  - AWS Fault Injection Service
  - Amazon CloudWatch
  - Amazon Route 53 Application Recovery Controller
  - AWS Elastic Disaster Recovery
  - AWS Backup

  Risk management and audit

  - AWS Cloud Audit Academy
  - AWS Artifact
  - AWS Audit Manager
  - AWS Security Hub

- AWS Resilience Hub
- AWS Config
- AWS Trusted Advisor
- AWS Security Assurance Services

Security of cloud workloads

- AWS Identity and Access Management (IAM)
- Amazon GuardDuty
- Amazon Inspector
- AWS Security Hub
- AWS Config
- AWS Shield and Shield Advanced
- Amazon CloudWatch
- AWS CloudTrail
- AWS Key Management Service (AWS KMS)
- AWS Professional Services

- Review the use of AWS Game Days, Security Incident Response Simulation and other practical testing exercises to validate and optimize the operational resilience of cloud deployments.

- Consider using AWS Enterprise Support to effectively manage, monitor, analyze, and report on usage of AWS services, as well as receive proactive planning, architectural reviews, and consultative guidance from AWS.

- Contact your AWS representative to discuss how the AWS Partner Network, and AWS Solution Architects, Professional Services teams, and training instructors can assist with your cloud adoption journey.

Further Reading

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

- AWS Security and Compliance Quick Reference Guide AWS has many features to assist FEs in aligning with compliance objectives for regulated workloads in the AWS Cloud. These features can help FEs achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry 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 AWS SRA 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 the customer's AWS accounts, and how they interact with other security services. This overall architectural guidance complements detailed, service-specific recommendations such as those found on AWS Security Documentation.

- The AWS Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help FEs 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 Cloud services and specifically, applying the Shared Responsibility Model to their regulatory requirements. FEs 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 AWS Cloud offerings conformance to NIST CSF risk management practices (that is, security of the cloud). FEs can use NIST CSF and AWS resources with their risk management frameworks.

For more information, refer to the Security Learning whitepapers