AWS guide to the ECB Guide on outsourcing cloud services to cloud service providers

May 2026

Notices

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

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 AWS guide (AWS Guide) helps financial entities (FEs) align their AWS cloud adoption with the European Central Bank (ECB) Guide on outsourcing cloud services to cloud service providers (ECB Guide). It explains how FEs can maintain control of their data and applications while taking advantage of AWS's global infrastructure and comprehensive security capabilities. It details AWS's approach to critical areas like business continuity, disaster recovery, and cyber resilience, and provides further information and guidance on how FEs architecture of their solutions and information and communication technology (ICT) considerations could contribute to meeting regulatory expectations and industry good practice.

The AWS Guide is structured in two parts. The first part provides a general overview of AWS's global infrastructure, comprehensive security capabilities and related elements. The second part is mapping the different elements of the ECB Guide against AWS services and documentation.

AWS empowers customers to maintain complete control over their data and applications while benefiting from AWS's proven expertise in securing and operating global cloud infrastructure. Through the AWS Shared Responsibility Model, AWS handles the security and resilience of the cloud itself, including the physical infrastructure, hardware, software, networking, facilities, and AWS services; while customers maintain control over the security and resilience of their applications running in the cloud, including their data, identity and access management configurations, application code, and operating systems.

Introduction

The increasing adoption of cloud services by FEs in the European Union is subject to regulatory oversight to ensure operational resilience and data security. The EU Digital Operational Resilience Act (DORA), which applies since January 2025, establishes legally binding requirements for FEs regarding their use of information and communication technology (ICT), including cloud services.

To support FEs in implementing DORA requirements, the European Central Bank (ECB) published the ECB Guide. This AWS Guide aims to provide clarity on supervisory expectations and good practices for effective cloud outsourcing. While the ECB Guide represents regulatory guidance rather than direct legal requirements, it provides the ECB's interpretation of how FEs should implement their legal obligations under DORA and related EU regulations.

This AWS Guide provides guidance for FEs seeking to adopt AWS cloud services in a manner aligned with the ECB Guide's supervisory expectations. It maps AWS

capabilities, certifications, and good practices to the key areas discussed in the ECB Guide, helping FEs and their advisors understand how AWS can support their regulatory compliance efforts.

NOTE: Some referenced white papers may carry the marking “This whitepaper is for historical reference only. Some content might be outdated and some links might not be available.” In those cases, we have opted to include the references because the information is still useful. As with any guidance, customers should exercise judgment and review before applying.

1. General overview

1.1. 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 FEs using AWS services need to comply with industry-specific regulatory obligations and internal requirements regarding operational resilience.

At AWS, we define *resilience* as the ability of an application to resist or recover from disruptions, including those related to infrastructure, dependent services, misconfigurations, and transient network issues.

Resilience is a shared responsibility between AWS and the customer. The AWS Shared Responsibility Model for Resiliency is fundamental to understanding the respective roles of AWS and its customers within the context of cloud services and operational resilience.

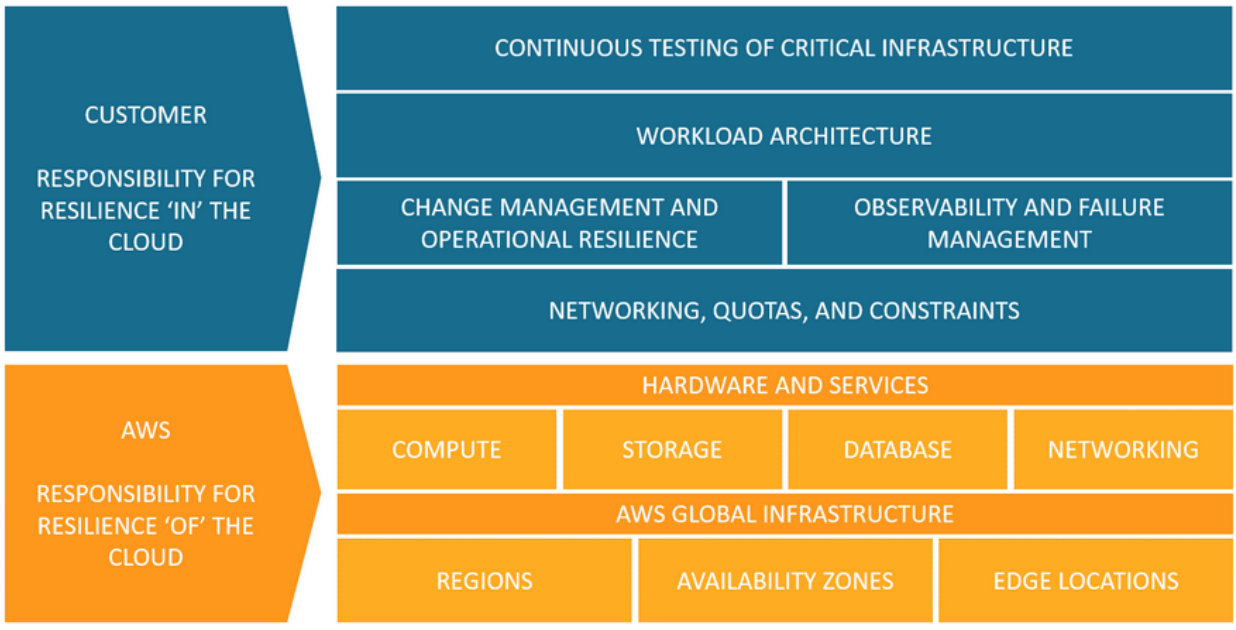

Figure 1: AWS Shared Responsibility Model for Resilience

AWS responsibility: resilience 'of' the cloud

AWS is responsible for ensuring that the AWS services used by customers are consistently available and ensuring that AWS is prepared to handle a wide range of events that could affect our cloud infrastructure, services, and operations. AWS handles the resilience of the cloud itself, including the infrastructure components, hardware, software, networking, facilities, and AWS services.

AWS infrastructure and services are designed to enable customers to build highly resilient workload architectures. AWS uses commercially reasonable efforts to make the AWS infrastructure and services available, and to ensure service availability meets or exceeds AWS Service Level Agreements (SLAs).

Customer responsibility: resilience 'in' the cloud

AWS customers are responsible for designing, testing, deploying, and operating their applications on AWS in a manner that achieves the availability and resilience they need, including the resilience of their software design and their operations.

The scope of a customer's responsibility depends upon the AWS services that they select. For example:

- A service such as Amazon Elastic Compute Cloud (Amazon EC2) requires the customer to perform resilience configuration and management tasks such as deploying EC2 instances across multiple locations (such as AWS Availability Zones), implementing self-healing architectures using services such as Amazon EC2 Auto Scaling, and using best practices to architect resilient workloads for applications installed on the EC2 instances.
- For managed services such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, 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 IAM tools to apply the appropriate permissions.

How customers can maintain resilience 'in' the cloud

Customers should carefully consider the AWS services they choose because their responsibilities vary depending on the services used, the integration of those services into their information and communication technology (ICT) environment, and applicable laws and regulations. The AWS Shared Responsibility Model provides the flexibility and customer control that allows customers to architect workloads according to their resilience objectives.

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 their 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 content 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.

- The AWS Well Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads. AWS Well Architected is built around six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability.
- The AWS Cloud Adoption Framework (AWS CAF) leverages AWS experience and best practices to help customers digitally transform and accelerate their business outcomes through innovative use of AWS. AWS CAF groups its capabilities in six perspectives: Business, People, Governance, Platform, Security, and Operations.

For more information on operational resilience, customers may refer to Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond and Disaster Recovery of Workloads on AWS: Recovery in the Cloud. Additionally, they may contact their AWS representative to discuss how the AWS FSI Compliance team, the AWS Partner Network, as well as AWS Solution Architects, Professional Services teams, and Training instructors can assist.

How AWS provides 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, or certifications such as ISO 22301

which provides assurance on AWS's commitment to business continuity and resilience of AWS global services.

The AWS compliance programs are 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 outputs of 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. Customers can use this information to perform their control evaluation and verification procedures.
- **Monitoring** through security controls that allow AWS to demonstrate compliance with global standards and best practices.

1.2. AWS Compliance Programs

AWS customers can review and download reports and details about controls by using AWS Artifact, the automated compliance reporting tool available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS's security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

AWS has obtained certifications and third-party attestations for a variety of specific industries. The following are of particular importance to FEs:

- **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 resilience of AWS global services. For more information or to download the AWS ISO 22301 certification, see the ISO 22301 Compliance webpage.

- **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 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:** An attestation supported by the German government and introduced in Germany by the Federal Office for Information Security (BSI). Cloud Computing Compliance Criteria Catalogue (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 further details, see the AWS C5 webpage.
- **Pinakes:** A cybersecurity control framework from a Spanish banking association, Centro de Cooperación Interbancaria (CCI). The framework helps Spanish FEs monitor cybersecurity controls of service providers they rely on, incorporating requirements from the EBA guidelines and DORA. For more information about AWS and Pinakes, see the AWS Pinakes 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.

1.3. AWS Global 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 (Region(s)). Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity; all housed in separate facilities (Availability Zones). These Availability Zones offer customers the ability to operate

applications and information and communication technology (ICT) resources such as databases, which are more highly available, fault tolerant, and scalable than what is typically achieved in a traditional, on-premises environment. Customers can learn more about these topics by downloading our whitepaper on Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond.

Customers choose the Region in which their content and servers are located. This allows customers to establish environments that meet specific geographic or regulatory requirements. Additionally, customers can either select a single Region approach, or implement a multi-Region architecture establishing primary and backup environments in a location or locations of their choice, depending on their business continuity and disaster recovery objectives. AWS provides fault isolation boundaries, such as Availability Zones, Regions, control planes and data planes. This architecture allows customers to design and deploy applications across multiple locations to achieve their desired levels of availability and fault tolerance. More information on our disaster recovery recommendations is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

All Regions are designed, built, and validated against rigorous compliance standards, providing high levels of security and resilience for customers. All Regions are validated against applicable national and global data protection laws. The IT infrastructure and services that AWS provides to its customers is designed and managed in alignment with best security practices and a variety of IT security standards.

1.4. 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 customers 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, customers 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 customers can assess controls, accelerating the compliance review process.

The table that follows presents the most common due diligence criteria we have identified in interactions with FEs and associated considerations for using AWS.

Due diligence criteria	Customer 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.
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 customers manage events in progress and provides proactive notification to help customers plan for scheduled activities.
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 customers 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 customers.

1.5. Additional support

AWS Enterprise Support

AWS Enterprise Support builds on 15+ years of experience helping organizations accelerate innovation and cloud operations with AI-powered capabilities. Customers' designated Technical Account Manager provides strategic guidance and deep AWS knowledge. Get intelligent troubleshooting through AI-powered assistance with direct engagement of AWS Support Engineers for rapid resolution. Automated security monitoring, triage, and proactive analytics combine with human expertise to transform cloud challenges into growth opportunities.

Security is strengthened through AWS Security Incident Response, which helps customers prepare for, respond to, and recover from security events faster and more effectively. The service streamlines every step of the security incident response lifecycle through automated security finding monitoring and triage, AI-powered investigation, and containment capabilities. When specialized expertise is required, Security Incident Response gives customers direct 24/7 access to Security Incident Response engineers, who respond to customers' requests within minutes.

AWS Professional Services

AWS Professional Services combines specialized solutions, deep industry expertise, and dedicated centers of delivery excellence to help organizations design, build, migrate, and manage their AWS workloads and applications. Businesses get unique access to AWS innovations, proven frameworks, and specialized capabilities to accelerate timelines, reduce risk, and deliver faster time to value. AWS Professional Services can supplement customers' teams with specialized skills and experience to help them realize their desired business outcomes when using the AWS cloud.

Working with AWS Partners, the Professional Services team offers customers flexibility in how they build and scale their AWS implementations. This collaborative approach ensures organizations can access the right mix of technical expertise, industry knowledge, and ongoing support to meet their specific needs.

AWS Security Assurance Services

AWS Security Assurance Services (AWS SAS) helps organizations streamline their path to compliance while maintaining robust security standards in the cloud by combining specialized solutions, deep industry expertise, and dedicated centers of delivery excellence to help organizations design, build, migrate, and manage their AWS workloads and applications. AWS SAS helps customers achieve, maintain, and automate compliance in the cloud by connecting audit standards to AWS service-

specific features and functionality. The team supports customers building on frameworks including ISO 27001, SOC 2, DORA, NIS2, NIST, and PCI DSS. As a PCI-QSAC (Payment Card Industry-Qualified Security Assessor company) and HITRUST External Assessor Firm, AWS SAS delivers specialized expertise that bridges the gap between cloud technology and regulatory requirements across international markets.

AWS Partner Network

The AWS Partner Network is a global community of AWS trusted cloud partners with diverse expertise who can assist customers on their cloud journey.

- AWS Partners with the Resilience Competency - provide solutions and guidance to help improve the availability of customers' critical workloads on AWS.
- AWS Partners with the Security Competency - offer security solutions and have demonstrated technical expertise and customer success with securing workloads on AWS.

AWS Training and Certification

Developing cloud skills and expertise across the workforce is a critical first step as organizations continue their cloud journeys. While cloud maturity is an iterative process, effective training and enablement is crucial for the success of this transformative journey. AWS provides training resources and strategies that organizations can leverage to upskill their workforce across key topics including cloud security and resilience.

2. Supervisory expectations in the ECB Guide

The following tables provide considerations for customers to meet expectations set out in the ECB Guide. The tables are organized as follow:

- **Summary of expectations.** Identifies the supervisory expectations from the ECB Guide. This is not the original text from the ECB Guide, but a summary prepared by AWS of the content of the ECB Guide.
- **Considerations for FEs that are AWS customers.** Provides considerations and lists AWS services and resources to help FEs align to the supervisory expectations in the ECB Guide within their scope of the AWS Shared Responsibility Model.
- **Additional resources.** Lists resources that help FEs implement the supervisory expectations described in the ECB Guide.

Note that the considerations and resources that follow do not guarantee compliance. These tables consist of a non-exhaustive set of summarized provisions. Customers must maintain compliance by employing methods appropriate to their specific operating environment. This can include using various configuration options provided by AWS services, integrating third-party solutions, where necessary, and implementing other necessary functions as required. Customers are strongly advised to refer to the ECB Guide to understand the full set of expectations from the ECB. This document does not constitute legal or compliance advice. Customers should consult with their legal and compliance teams.

Section 2. Supervisory expectations

2.1. Governance of cloud services

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
2.1.1 Full responsibility of supervised entities Supervised entities must establish a governance framework for cloud service outsourcing with clearly defined roles and responsibilities. While both the Cloud Service Provider (CSP) and supervised entity share operational responsibilities, the supervised entity's management body retains ultimate ICT risk accountability under Article 5(2) of DORA. Industry good practice for outsourcing ICT services requires that financial institutions apply the same level of diligence regarding risk management practices, processes, and controls—including ICT security—as if they had retained those services in-house, consistent with the European Central Bank's supervisory expectations.	FEs are responsible for defining their operational process model for managing systems, databases, and services, as well as the ICT risk management processes. AWS provides services and guidance to help FEs meet operational requirements, but FEs retain responsibility for developing and implementing their own policies and procedures for ICT operations. FEs can refer to the AWS Shared Responsibility Model to understand allocation of responsibilities between customers and AWS for security and compliance, and the Shared Responsibility Model for Resiliency to understand allocation of responsibilities for resilience. FEs should document their cloud governance framework, including management body oversight mechanisms, risk assessment processes, and decision-making authorities for cloud-related matters. This governance framework should acknowledge that while AWS operates the underlying cloud infrastructure and provides security controls at the infrastructure level, the FEs retain responsibility for configuring services appropriately, managing access controls, protecting data, ensuring business continuity, and demonstrating regulatory compliance to supervisors. AWS provides mechanisms that enable FEs to exercise effective oversight of their cloud arrangements, thereby demonstrating to supervisors that they maintain ultimate accountability despite operational ICT outsourcing. The AWS Well-Architected Framework – Management and Governance Cloud Environment Guide routes customers in implementing comprehensive logging, monitoring, and alerting architectures that provide the visibility necessary for management bodies to understand the operational status of their cloud environments and	FSIOPS1 - Define risk management roles for cloud FSIOPS2 - Complete an operational risk assessment AWS Well-Architected Framework – Management and Governance Cloud Environment Guide AWS CAF: Governance Perspective

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	make informed risk decisions. whether they remain within acceptable risk parameters. The AWS Well-Architected Framework Management and Governance Cloud Environment Guide also provides guidance on implementing technical controls that enable FEs to maintain operational control over their cloud environments despite relying on AWS for the underlying infrastructure. The principle of equivalent risk management set out under Section 2.1.1 of the ECB Guide establishes that outsourcing does not diminish the financial institution's ultimate accountability for operational resilience, data protection, or regulatory compliance. FEs using AWS services can directly access and download, through the AWS site, copies of attestations and certifications issued by external auditors to AWS as part of the AWS information security program. For information about independent monitoring of AWS, refer to *2.5.1 Independent monitoring of CSPs*.	
2.1.2 Ex ante risk assessment Under Article 28(4) of DORA, supervised entities must conduct an ex-ante risk assessment before entering cloud outsourcing arrangements. Good practices include analyzing control processes and their integration, assessing the CSP's ability to provide required information, verifying the CSP's control implementation, evaluating internal expertise and resources, and assessing sub-outsourcing chain risks for	AWS recognizes the importance of supporting customers through their regulatory requirement and has developed comprehensive resources, documentation, and engagement models designed to facilitate thorough ex ante risk assessments. AWS's commitment to transparency, extensive compliance certifications, and detailed control documentation enables FEs to conduct rigorous evaluations efficiently. The AWS Compliance Programs are designed to help customers understand the controls in place at AWS to maintain security and compliance of the cloud, their relevance to the AWS services customers use, and how those controls have been validated. Within the AWS Compliance Program portal, customers can find compliance certifications and attestations relating to regulations and standards. Compliance certifications and attestations are assessed by a third-party independent auditor and result in a certification, audit report, or attestation of compliance. Customers remain responsible for complying	Security, Identity, and Compliance on AWS AWS Compliance Programs Access AWS security and compliance reports AWS Trust Center AWS Pricing How AWS Pricing Works

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
critical or important functions. A comprehensive ex ante risk assessment should also incorporate evaluation of vendor lock-in and the potential challenges in identifying alternative providers during exit scenarios; data storage and processing risks; region-specific risks related to political stability and jurisdictional characteristics of countries where services are provided and data are stored; risks of quality degradation or price increases and multi-tenant environment risks.	with applicable laws and regulations. To understand how customers can use AWS services to protect their data and help them maintain security in the cloud, customers can visit the AWS Trust Center. The Trust Center explains in clear terms how we safeguard customer information through our security practices, operational controls, and data protection measures. Customers will also learn about our privacy commitments, how we manage operator access, and our approach to digital sovereignty. The following sections cover additional topics about *ex ante risk assessment*: • Box 1: Learn how you can reduce concentration and technology lock-in risk when running workloads on AWS. • Section 2.2 - *Availability and resilience of cloud services*: Learn how to back up your data and prepare for events, including cyber incidents like ransomware. Discover how to architect your critical applications on AWS depending on your operational resilience requirements. • Section 2.3 - *ICT and data security, confidentiality, and integrity*: Learn how to help prevent cyber incidents, meet your digital sovereignty needs, and use AWS service privacy features. This section also covers subcontracting and how AWS designs its systems to prevent unauthorized access by AWS personnel to customer data. • Section 2.4 - *Exit strategies and termination rights*: Learn how to design your exit strategy and migrate your data to or from AWS. AWS provides services on a pay-as-you-go model, allowing customers to only pay for the AWS services they need and use, and AWS does not charge termination fees. Customers also have the option to use our reserved instances, offering them a discount.	

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
Box 1 Assessment of concentration risk and provider lock-in risk Article 28(4)(c) of DORA requires ex ante risk assessments to evaluate contractual arrangements and ICT concentration risk. The ECB recommends evaluating risks relating to provider lock-in, pricing models, audit, function concentration, and sub-provider visibility.	When running workloads on AWS, FEs can reduce concentration and technology lock-in risk as follows: 1. FEs can take advantage of the AWS global infrastructure and the fault isolation boundaries it provides. For example, FEs can implement business continuity and disaster recovery plans that take advantage of multiple AWS Regions as described in *2.2.1 Holistic perspective on business continuity measures for cloud solutions*. FEs can architect applications to the required level of operational resilience as described in *2.2.2 Proportionate requirements for critical or important functions*. 2. FEs can flexibly opt in or out of using individual AWS services as their needs change, enabling highly granular control over service adoption and discontinuation. AWS offers over 200 fully featured services. Offering customer choice and freedom is a core principle throughout AWS. AWS does not have mandatory minimum commitments, or mandatory long-term contracts. Long-term contracts are offered as a choice for the customer's convenience. For additional provisions relating to termination rights for European FEs refer to *2.4.1 Termination rights*. 3. AWS provides services on a pay-as-you-go model. FEs can select their AWS services with visibility on the associated fees. AWS services are priced independently and transparently. FEs can also save money by using the AWS reservation model. With the pay-as-you-go model, FEs will pay only for the services they need, allowing them to focus on innovation and invention while reducing procurement complexity and maintaining business flexibility. 4. FEs can use managed open source services such as Amazon Elastic Kubernetes Service (EKS), Amazon Relational Database Service (RDS) with PostgreSQL, MariaDB or MySQL engines, and Amazon OpenSearch Service. AWS supports open-source projects, foundations, and partners, working closely with the	Unpicking Vendor Lock-in Open source at AWS AWS Pricing Containers on AWS Data porting on AWS Cloud Data Migration AWS Online Register of Data Formats AWS EU Data Act Addendum

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	open-source community, contributing to open-source projects, and building services that are compatible with open-source tools. 5. AWS works with independent software vendors (ISVs) who have permitted the use of their product on AWS, enabling customers to bring their own license (BYOL) for the BYOL terms to apply on AWS. This helps customers reduce switching costs when moving away from AWS. AWS License Manager makes it easier to bring existing software licenses from vendors such as Microsoft, SAP, Oracle, and IBM to AWS, and centrally manage these licenses across AWS and on-premises environments. 6. FEs can design for application portability by keeping system components independent from each other for example by using decoupled architectures and container technologies to isolate code from the ICT environment it's stored in. AWS offers FEs the possibility to choose the right AWS service for their workload, from small experiments to critical production applications. As new AI technologies have emerged, AWS is supporting emerging interoperability protocols, such as the Model Context Protocol (MCP), which enables AI applications to securely connect with data sources across different systems, and Agent-to-Agent protocol (A2A) which enable standardized communication between AI agents across different providers. 7. AWS services provide APIs which allow you to export data in a structured format, and AWS provides many tools and documented techniques to support both data migration into and out of AWS. For further information on migrating into or out of AWS see in *2.4 Exit strategies and termination rights*. See *2.4.2 Components of the exit strategy and alignment with the exit plan* for further information on data portability and customer control over their data lifecycle, including on migration processes, provider switching or data repatriation to on-premises systems. For information regarding the other topics mentioned in *Box 1* of the ECB	

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	Guide, refer to section *2.1.2 Ex ante risk assessment*.	
2.1.3 Consistency between a supervised entity's cloud strategy and its overall strategy Article 6(3) of DORA requires supervised entities to minimize ICT risk through appropriate strategies, policies, procedures, protocols, and tools. Article 28(2) mandates a strategy covering ICT third-party risk, specifically cloud service provider outsourcing.	The AWS Cloud Adoption Framework: Governance Perspective whitepaper provides guidance on risk management and governance in the context of cloud adoption. The Governance perspective focuses on helping FEs plan their cloud initiatives while maximizing organizational benefits and minimizing transformation-related risks. It supports customers in developing cloud strategies and architecting cloud-based systems, ensuring consistency across organizational risk practices.	AWS Cloud Adoption Framework: Governance Perspective

2.2. Availability and resilience of cloud services

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
2.2.1 Holistic perspective on business continuity measures for cloud solutions Articles 85(2) of Capital Requirements Directive (CRD) and 11(1) of DORA require contingency, business continuity, and disaster recovery plans. When using cloud services for critical or important functions, supervised entities	AWS provides FEs with the ability to implement their own robust business continuity and disaster recovery plans. This includes the ability to create recovery ICT systems and backups that are physically and logically segregated from the source ICT systems. The AWS Shared Responsibility Model establishes that customers are responsible for operating and recovering applications during failures or disasters. AWS provides the infrastructure and tools available for FEs that need to build their systems focusing on resilience, including fault isolation boundaries, such as Availability Zones, Regions, control planes and data planes. FEs can use these features to create their own ICT recovery systems, backups, and procedures that are separate from their source	REL 9 - Back up data REL 13 - Plan for disaster recovery (DR) AWS Fault Isolation Boundaries Establishing Your Cloud Foundation on AWS - Business Continuity Disaster Recovery of Workloads on AWS: Recovery in the Cloud

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
must ensure business continuity, resilience, and disaster recovery capabilities.	systems. When planning for service continuity, FEs have the possibility to adopt a scenario-based approach rather than categorizing plans as short-term or long-term: • For availability-impacting scenarios, FEs can: Plan for environmental events (floods, earthquakes, tornados), physical failures (server crashes, disk failures, network cuts), and software issues (bugs, deployment problems, traffic spikes). Address these using both high availability and disaster recovery strategies that leverage AWS global infrastructure and its fault isolation boundaries. • For supplier and third-party risk scenarios, FEs can: Prepare for vendor exits, bankruptcies, or sanctions through contracts and migration planning. Create exit plans that outline how FEs will move to another provider if needed. For more details on exit planning, see sections: *2.4.2 Components of the exit strategy and alignment with the exit plan* and *2.4.3 Granularity of exit plans*. For availability-impacting scenarios, AWS provides FEs 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 AWS Regions as well as across multiple Availability Zones (AZs) within each AWS Region. Consult Disaster Recovery of Workloads on AWS: Recovery in the Cloud for guidance on implementing a disaster recovery strategy as part of your business continuity planning. AWS Backup is designed to help customers centrally manage and automate backups across AWS services and third-party applications. FEs can use AWS Backup Vault Lock to manage backups using immutable storage, and logically air-gapped vaults to provide increased security beyond a standard backup vault. These capabilities help FEs protect data from inadvertent deletion, cyber events such as ransomware compromise,	Cyber event recovery in financial services

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	and other threats. AWS provides guidance on building data vault architectures for cyber event recovery in financial services. AWS Elastic Disaster Recovery (AWS DRS) is designed to help customers minimize downtime and data loss with fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery. Amazon Application Recovery Controller provides insights into whether applications and resources are ready for recovery and is designed to help customers manage and coordinate recovery for their applications across AWS Regions and AZs.	
2.2.2 Proportionate requirements for critical or important functions Supervised entities must adopt appropriate resilience measures using risk-based and proportionate approaches per Article 85(2) of CRD and Article 6(8) of DORA.	FEs can achieve their objectives for operational resilience by taking advantage of the AWS global infrastructure and the fault isolation boundaries it provides. AWS recommends the following to contribute to FEs resilience objectives: • Understanding the AWS Shared Responsibility Model for Resiliency • Selecting AWS services that align with the resilience targets of the workload. • Architecting for reliability, observability, operations, and static stability. • Adopting the disaster recovery design pattern most appropriate for the applicable workload (for example, Backup & Restore, Pilot Light, Cold Standby, Warm Standby, or Active-Active) • Planning for gray failures, which are failures observed differently by different entities. • Making sure that failover mechanisms themselves are highly available. Whenever possible, AWS recommends that FEs use	REL - Reliability Pillar OPS - Operational Excellence Pillar FSIREL - Reliability AWS Fault Isolation Boundaries Advanced Multi-AZ Resilience Patterns AWS multi-Region fundamentals Static stability using Availability Zones Resilience lifecycle framework Resilience analysis framework Availability and Beyond: Understanding and Improving the Resilience of Distributed Systems on AWS

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	data plane functions for their failover mechanisms. • Testing reliability and regularly provide time for analysis of operations activities, analysis of failures, experimentation, and making improvements. • Learning from incidents and using the insights gained to make improvements incrementally. AWS Resilience Hub helps customers, including FEs, define, validate, and track the resilience of their applications on AWS from a single place. AWS uses fault isolation to contain system failures within defined boundaries. Customers, including FEs can design workloads to take advantage of these predictable boundaries, which include partitions, Regions, Availability Zones, control planes, and data planes. Depending on the applications, resilience can be achieved using an independent and physically separate Availability Zones within a single AWS Region. FEs can also implement a multi-Region architecture depending on criticality of the applications or objectives. The AWS Prescriptive Guidance on AWS multi-Region fundamentals provides guidance on common use cases and explains key concepts for design, development, and deployment. AWS services are designed for static stability, which means they are designed to stay resilient even when their dependencies become impaired. For example, the data plane is designed to maintain its existing state and continue working even if the control plane becomes impaired. Customers can design their workloads for static stability by reducing or eliminating control plane and cross-Region dependencies at runtime. While some global services have single-Region control plane operations, their data planes follow similar isolation and independence principles as Regional AWS services. This allows the use of services in a given Region while maintaining static stability. To date, the AWS global infrastructure includes 39 Regions. Regions themselves are isolated and independent from other Regions, with the	Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond AWS Service Level Agreements (SLAs)

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	exception of global service control planes. Each Region has at least three Availability Zones that are designed to operate independently. An Availability Zone consists of one or more discrete data centers with separate power, networking, and connectivity infrastructure. Availability Zones within a Region are: • Located up to 60 miles (100 km) apart to prevent correlated failures • Close enough for synchronous replication with single-digit millisecond latency • Protected from simultaneous failures due to utilities, natural disasters, or other disruptions • Equipped with independent generators, cooling equipment, and power substations AWS deploys service updates to Availability Zones at different times to prevent correlated failures. Regions operate independently from each other, except for global services. For guidance on recovery, including cyber event recovery, refer to *2.2.1 Holistic perspective on business continuity measures for cloud solutions*.	
2.2.3 Oversight of the planning, establishment, testing and implementation of a CSP's disaster recovery strategy Supervised entities must implement and test a robust disaster recovery strategy.	AWS provides global infrastructure locations with fault isolation boundaries to which customers can recover, as well as tools and services to assist with that recovery. FEs can review the Disaster Recovery of Workloads on AWS: Recovery in the Cloud for guidance on implementing a disaster recovery strategy as part of their business continuity planning and regulatory and compliance obligations AWS provides training resources and strategies that organizations can leverage to upskill their workforce across key topics including cloud security and resilience. For more information on operational resilience, refer to Amazon Web Services' Approach to Operational Resilience in the	AWS Fault Isolation Boundaries Disaster Recovery of Workloads on AWS: Recovery in the Cloud Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	Financial Sector & Beyond. For further information refer to *2.2.1 Holistic perspective on business continuity measures for cloud solutions*. For guidance on how customers can engage directly with AWS on matters of audit, compliance, and security, refer to *2.5 Oversight, monitoring and internal audits*.	

2.3. ICT and data security, confidentiality and integrity

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
2.3.1 Establishment of adequate data security measures Supervised entities must implement adequate security measures, including cryptographic protection measures, based on data classification and ICT risk assessments.	FEs are responsible for defining their ICT security policies, procedures, protocols, and tools as part of their risk management framework. Customers can adopt a culture of security by establishing norms and practices that align with keeping the enterprise secure. Consult the Security Pillar of the AWS Well-Architected Framework for guidance on current recommendations in the design, delivery, and maintenance of secure AWS workloads. The Security Pillar describes how customers can simplify their security control operations using AWS services such as AWS Control Tower, AWS Security Hub, AWS Config and Amazon GuardDuty. FEs should apply permission guardrails to enforce mandatory controls around security, operations, and compliance. Consult AWS Prescriptive Guidance Implementing security controls on AWS for guidance on building a security governance strategy based on a policy, control objectives, standards, and security controls; and the AWS Security Reference Architecture (AWS SRA) for a holistic set of guidelines on deploying AWS security services in a multi-account environment. AWS's cryptographic services use a wide range of encryption and storage technologies that can assure the confidentiality and integrity of customer	SEC - Security pillar FSISEC - Security Implementing security controls on AWS AWS Security Reference Architecture (AWS SRA) AWS Key Management Service Cryptographic Details Zero trust on AWS Data perimeters on AWS Data masking 5 Steps to Building a Culture of Security AWS Skill Builder – Security Champion Knowledge Path

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	data. • To protect data at rest, most AWS services provide encryption capabilities using AWS Key Management Service (AWS KMS). To ensure data is encrypted using keys that are unique to customer workloads, customers can use KMS customer managed keys. Customer managed keys provide customers with full control over establishing and maintaining their key policies, enabling and disabling them, rotating their cryptographic material, and scheduling them for deletion. • To protect data in transit, customers can use AWS service endpoints designed to provide encryption of data in transit using a minimum TLS version of 1.2. Customers can enforce their TLS standards in their own applications using AWS services such as Elastic Load Balancing (ELB), Amazon CloudFront, and Amazon API Gateway. Customers can manage certificates using AWS Certificate Manager (ACM) and AWS Private Certificate Authority. • To protect data in use, customers can follow AWS guidance on separating workloads using accounts, segmenting networks into different layers, and granting least privilege access. Customer can also review the AWS approach to confidential computing and the protections afforded by the security design of the AWS Nitro System. To further strengthen customers' posture and reduce surface area, customers should adopt zero trust architectures and implement data perimeters on AWS. FEs can also use data masking or tokenization on AWS to help protect sensitive data fields. To simplify cryptography operations for payment applications hosted in the cloud, customers can use AWS Payment Cryptography. FEs may conduct ICT security testing of their AWS environment in accordance with the AWS Customer Support Policy for Penetration Testing. AWS Security Agent is a frontier agent that proactively secures customer	AWS Customer Support Policy for Penetration Testing

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	applications throughout the development lifecycle. The agent conducts automated security reviews based on customer requirements and performs on-demand penetration testing to discover and report verified security risks customized to a customer's application. The information in this section contributes to helping protect customers from security threats, including cyber events such as ransomware. For information on recovering from cyber events, refer to *2.2.1 Holistic perspective on business continuity measures for cloud solutions*.	
2.3.2 Risks stemming from the location and processing of data Under DORA regulations, ICT response and recovery plans must consider scenarios of instability, including where third-party service providers operate and where data is stored. Financial institutions should maintain a list of approved countries for data storage and processing based on their data classification requirements.	With AWS, customers own their data, control their location, and control who has access to it. AWS will not move or replicate customer's content outside customer's chosen Region(s) without customer's agreement. Customers have full control over who can access their data. AWS does not use customer data or derive information from it for marketing or advertising purposes. AWS prohibits, and AWS systems are designed to prevent remote access by AWS personnel to customer data for any purpose, including service maintenance, unless that access is requested by customer, is required to prevent fraud and abuse, or to comply with law. For more information about AWS operator access, see section *2.3.4 Identity and access management policies for cloud outsourcing arrangements*. AWS provides guidance, compliance evidence, and contractual commitments to help customers meet their compliance and regulatory requirements using AWS services. Our AWS Digital Sovereignty Pledge, introduced in 2022, offers customers advanced sovereignty controls and features available in the cloud. AWS continuously expands these capabilities so customers can meet their digital sovereignty needs without compromising on the performance, innovation, security, or scale of the AWS Cloud. AWS is transparent about how AWS services process customers' data and provide capabilities that allow customers to encrypt, delete, and monitor the processing of their data. All AWS services support encryption, and most services also support encryption with customer managed keys	Data Protection & Privacy at AWS Digital Sovereignty at AWS Data Privacy FAQs Privacy Features of AWS Services AWS Sub-processors

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	that AWS is not able to access. When AWS engages subcontractors, AWS follows strict processes to protect the AWS Network and maintain service continuity. AWS thoroughly evaluate potential subcontractors before engagement, reviewing relevant factors which may include, among others, their corporate and ownership structure, financial statements, credit, internal policies, and skill and suitability of the subcontractor's personnel. AWS monitors subcontractors throughout their service period and provide information about its subcontractors in the AWS Sub-outsourcing List / AWS Digital Operational Resilience Act (DORA) Subcontracting List, available from AWS Artifact. FEs can subscribe to email notifications about any changes to the list of the AWS subcontractors. Regulated customers subject to DORA running regulated workloads on AWS can enter into a specific Financial Services Addendum (FSA), giving those regulated customers access to further information on AWS Sub-Outsourcing, in the FSA and via self-service information available on AWS Artifact. For information about AWS operator access, see *2.3.4 Identity and access management policies for cloud outsourcing arrangements*.	
2.3.3 Consistent inclusion of outsourcing assets in a supervised entity's inventory of ICT assets Under Article 8(1) of DORA, supervised entities must identify, classify, and document all ICT-supported business functions, roles, responsibilities, information assets, ICT assets, and their interdependencies regarding ICT risk. The ECB	FEs are responsible for defining their policies for managing their ICT assets, including their AWS resources. Customers can use AWS accounts to group resources belonging to distinct workloads. An AWS account acts as an identity and access management isolation boundary. An AWS account provides security, access, and billing boundaries for your AWS resources that can help you achieve resource autonomy and isolation. By design, all resources provisioned within an account are logically isolated from resources provisioned in other accounts, even within your own AWS environment. This isolation boundary provides you with a way to limit the risks of an application-related issue, misconfiguration, or malicious actions. If an issue occurs within one account, impacts to workloads contained in other accounts can be either reduced or eliminated. AWS accounts are uniquely	SEC 1 - Security foundations OPS 5 - Design for operations DL.EAC - Everything as code AWS account AWS account IDs Data Classification on AWS

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
recommends adopting a clear asset classification policy covering all ICT assets, including outsourced cloud services.	identified using AWS account IDs. FEs can use AWS Organizations to centrally manage and govern their multi-account AWS environment as they grow and scale their AWS resources. FEs can use AWS services to create and manage resources within accounts, such as compute instances, databases, and networks. The status of those resources is tracked by the relevant service within the boundary of a specified AWS account. AWS resources are uniquely identified using Amazon Resource Names (ARNs). To query or report on resources within FEs AWS accounts, FEs can use the relevant service's control plane APIs. FEs can also use the AWS Config service to assess, audit, and evaluate the configurations of resources across multiple services. FEs can apply tags to their resources to store metadata relating to individual resources such as data classification. For AWS services that generate ephemeral resources, such as ECS tasks configured to use automatic scaling in Amazon Elastic Container Service (Amazon ECS), the lifecycle of such resources is managed by the service itself within the boundary of a specified AWS account.	
2.3.4 Identity and access management policies for cloud outsourcing arrangements Cloud environment configuration must be clearly defined, agreed upon, and properly segregated between parties. A supervised entity's identity and access management (IAM) policy should extend to cloud assets and cover both technical	**Customer responsibilities** Customers maintain full control over the user and system identities in their AWS environment. AWS IAM Identity Center is designed to help customers connect their existing workforce identity source and centrally manage access to AWS. For users and workloads that require access to AWS, AWS Identity and Access Management (IAM) enables secure access through roles, instance profiles, identity federation, and temporary credentials. AWS recommends customers consult the Security Pillar of the AWS Well-Architected Framework for guidance on identity and access management on AWS. Consult Security best practices in IAM for a summary of AWS identity and access management recommendations, such as strong	SEC 2 - Identity Management SEC 3 - Permissions management Security best practices in IAM Zero trust on AWS Data perimeters on AWS Operator Access on AWS

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
and business users.	authentication and federation for human users, temporary credentials with IAM roles for workloads, and least-privilege access control policies. Apply permission guardrails to enforce mandatory controls around security, operations, and compliance. To further strengthen customers' posture and reduce surface area, adopt zero trust architectures and implement data perimeters on AWS. **AWS responsibilities** AWS implements security measures to help protect customer content. AWS systems are also designed to prevent access by AWS personnel to customer data for any unauthorized purposes. AWS commit to that in the AWS Customer Agreement and AWS Service Terms. AWS operations never require us to access, copy, or move your data without your knowledge and authorization. Many of the AWS core systems and services are designed with zero operator access. These services do not have any technical means for AWS operators to access customer data. Instead, systems and services are administered via automation and secure APIs that protect customer data from inadvertent or even coerced disclosure. AWS also apply the principle of least privilege to the posture of AWS systems and services, making sure AWS employees have access only to the minimum set of systems required to do their assigned task or job responsibility, and limit that access in time for only when such access is needed.	
Box 2 Access management, remote access and authentication of users Supervised entities must implement robust access management practices for cloud systems supporting critical or	**Customer responsibilities** AWS Identity and Access Management (IAM) enables secure access through roles, instance profiles, identity federation, and temporary credentials. Customers may consult Security best practices in IAM for a summary of AWS identity and access management recommendations, such as strong	SEC 2 - Identity management SEC 4 - Detection Operator Access on AWS

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
important functions, including strong multi-factor authentication (especially for users with privileged access), regular access reviews and re-certification processes, clear identification of business owners for accountability, and appropriate monitoring and logging of the CSP's access to the entity's data.	authentication and federation for human users, temporary credentials with IAM roles for workloads, and least-privilege access control policies. AWS Systems Manager Session Manager provides secure node access without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. To monitor and record account activity across customers AWS infrastructure, customers can use AWS CloudTrail. **AWS responsibilities** AWS personnel perform their operations through secured interfaces ensuring operators have up-to-date and secured workstations, FIPS-validated hardware security tokens, and are correctly authenticated. These interfaces provide AWS operators with temporary short-lived credentials, and also monitor all activity using mechanisms that cannot be over-ridden or bypassed. These secure operator interfaces permit only limited operations that do not disclose customer data and enforce multi-person approval for sensitive operations. Any access to systems that store or process customer data or metadata is logged, monitored for anomalies, and audited. AWS guards against any actions that would disable or bypass these controls. For further information on identity and access management, refer to *2.3.4 Identity and access management policies for cloud outsourcing arrangements*.	

2.4. Exit strategies and termination rights

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
2.4.1 Termination rights Under Article 28(7) of DORA,	FEs can flexibly opt in or out of using individual AWS services as their needs change, enabling highly granular control over service adoption and discontinuation. AWS offers over 200 fully featured services. Offering	AWS Cloud Security: Digital Operational Resilience Act

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
cloud outsourcing contracts must include clear termination rights for circumstances including persistently inadequate performance or significant contractual/legal breaches. For critical or important functions, contracts should include transition periods reducing disruption risk and enabling provider switching, insourcing, or decommissioning.	customer choice and freedom is a core principle throughout AWS. AWS does not have mandatory minimum commitments, or mandatory long-term contracts. Long-term contracts are offered as a choice. AWS has released a Digital Operational Resilience Act (DORA) Financial Services Addendum (FSA) which supplements the existing financial services addenda in order to reflect the contracting requirements of DORA. This addendum includes additional provisions relating to termination rights. Eligible customers can contact their AWS Account Manager to request the DORA FSA.	
2.4.2 Components of the exit strategy and alignment with the exit plan and **2.4.3 Granularity of exit plans** Under Article 28(8) of DORA, supervised entities should establish an overarching exit strategy with granular technical exit plans for cloud arrangements supporting critical or important functions. Transition plans must enable secure, complete data and application removal and transfer to alternative providers or in-house reincorporation.	FEs are in control of their exit planning and have freedom to move to another cloud services provider (CSP) should they choose to. FEs always retain ownership and control of their data, including where it is stored, how it is secured, and who has access to it. AWS services provide APIs which allow customers to export data in a structured format, and AWS provides many tools and documented techniques to support both data migration into and out of AWS. FEs can use the AWS Online Register of Data Formats to find AWS APIs that retrieve data from services. Since March 2024, AWS has waived data transfer out to the internet (DTO) charges (as a one-time transfer) when AWS customers want to move outside of AWS as part of a switch to another cloud provider or a switch to on premises operations. This follows the direction set by the European Data Act and is available to all AWS customers around the world and from any AWS Region. EU customers exercising a switch under the EU Data Act should review the criteria and process described in the AWS EU Data Act Addendum. AWS is actively engaged in efforts to facilitate switching between cloud providers, including through our support of the Cloud Infrastructure	Unpicking Vendor Lock-in Data porting on AWS Cloud Data Migration AWS Online Register of Data Formats

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
Exit plans should include critical milestones, required tasks and skillsets, time and cost estimates, and be regularly reviewed and tested.	Service Providers in Europe (CISPE) Cloud Switching Framework, which lays out guidance to assist providers and customers in the switching process. FEs could consider developing a framework that encompasses detailed documentation of migration processes, technical specifications, associated costs, and realistic timeframes for both provider switching and data repatriation to on-premises systems. The AWS Shared Responsibility Model serves as the foundational principle governing data portability obligations, with CSPs bearing responsibility for providing capabilities for data movement while customers retain ultimate ownership and control of their information. Customers can maintain control over critical decisions including storage format selection, geographic data residency, and the timing of data downloads or deletions. To validate provider capabilities, organizations can request demonstrations of data portability tools and migration services during the vendor evaluation process, ensuring these mechanisms function effectively under realistic conditions. The above considerations, combined with comprehensive agreements covering portability commitments, provide the operational enablement for enterprise cloud adoption while reducing technology lock-in risk. For further guidance on reducing concentration and technology lock-in risk, refer to *Box 1 Assessment of concentration risk and provider lock-in risk*. For information on business continuity and disaster recovery, refer to *2.2.1 Holistic perspective on business continuity measures for cloud solutions*.	

2.5. Oversight, monitoring and internal audits

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
2.5.1 Independent monitoring of CSPs Under Article 6(10) of DORA, supervised entities may outsource ICT risk management verification compliance tasks to intra-group or external undertakings but remain fully responsible. Verification of compliance itself cannot be outsourced, even for managed cloud services where CSPs maintain operations and security compliance. All contractual outsourcing arrangements—including intra-group arrangements—must accommodate reporting requirements for monitoring purposes, particularly for ICT services supporting critical or important functions, per Article 9 of Commission Delegated Regulation (EU) 2024/1773 supplementing DORA.	The AWS Compliance Programs are designed to help FEs understand the controls in place at AWS to maintain security and compliance of the cloud. For further details on AWS Compliance Programs, refer to *2.1.2 Ex ante risk assessment*. AWS offers a Financial Services Addendum (FSA) to financial services customers running regulated workloads. Additionally, AWS offers a Digital Operational Resilience Act (DORA) FSA which supplements the existing financial services addenda to reflect the contracting requirements of DORA. The AWS FSAs include contractual provisions to enable European customers to exercise their audit and access rights with AWS. AWS offers customers options to engage directly with AWS on matters of audit, compliance, and security, and provides the following mechanisms: • **Customer compliance briefings**: offer customers opportunities to engage directly with AWS on audit, compliance, and security matters. Compliance briefings support customers in addressing their security or compliance questions or concerns to AWS security and compliance specialists, who are appropriately qualified and knowledgeable AWS personnel. • **Community audit**: a pooled audit executed by a customer-chosen, reputable, and independent auditor performing testing of the AWS environment on behalf of a group of customers. These audits can be based on an existing AWS audit program such as C5, or by a set of controls driven by the members of the community. A community audit provides financial, regulatory, and time efficiencies to the institutions represented by the community, where all members have input into the audit scope while mutually benefitting from sharing the cost and effort of a single audit. Community audits help minimize audit duration while increasing overall control transparency, ensuring the highest bar of	AWS Compliance Programs AWS Artifact Cloud Audit Academy

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	assurance for the most security-conscious community members. Additionally, AWS Artifact is designed to provide access to AWS security and compliance reports. Cloud Audit Academy is designed to help current and upcoming auditors with the education and tools to audit for security in the cloud using a risk-based approach.	
2.5.2 Incident reports and contractual details Under Article 19(5) of DORA, supervised entities remain fully responsible for incident reporting requirements even when outsourcing these obligations to third-party service providers. Supervised entities should establish clear procedures, roles, and responsibilities for incident management with oversight capabilities to follow up on CSP incidents potentially affecting the entity. Incident reports must include sufficient details identifying affected services and enabling impact assessment on the entity's business.	For incident management guidance, refer to the Operational Excellence Pillar of the AWS Well-Architected Framework. This resource helps FEs architect workloads for observability and prepare for incident response. Although FEs independently assess whether AWS incidents trigger DORA reporting obligations, AWS Health provides ongoing visibility into FEs' resource performance and the availability of their AWS services and accounts. The AWS Health Dashboard shows FEs: • Current health status of AWS services • Reported service events across AWS Regions • Scheduled changes and planned lifecycle events • Events impacting their account or an account in their organization If FEs have a AWS Business Support+, AWS Enterprise Support, or AWS Unified Operations, they can create and manage support cases for technical assistance. • AWS Enterprise Support helps customers accelerate innovation, strengthens security, and streamlines cloud operations with AI-powered guidance and expert human support. Customers' designated Technical Account Manager provides strategic guidance and deep AWS knowledge. Customers get intelligent troubleshooting through AI-powered assistance with direct engagement of AWS Support Engineers for rapid resolution. The service combines automated security monitoring, triage, and proactive analytics with expert support. • Customers can also enroll in Unified Operations depending on	OPS 8 - Utilize workload observability SEC 4 - Detection FSIOPS 5 – Understand workload health FSIOPS 6 - Assess business impact of a cloud provider service event FSISEC12: Meet obligations for incident reporting to regulators Incident management on AWS AWS Health Compare AWS Support plans AWS Enterprise Support Unified Operations AWS Incident Detection and Response AWS Security Incident Response AWS Security Bulletins AWS Data Processing Addendum

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	their resilience requirements and criticality level of their enterprise operations. With Unified Operations, designated AWS specialists act as an extension of their team via their preferred collaboration channels, conducting workload reviews, providing strategic guidance, and optimizing performance through deep contextual knowledge. With 24/7 security and performance monitoring, we detect and mitigate incidents early while reducing alert volume. When a critical incident occurs, we respond within five minutes with context of customers' environment, to further shorten resolution time and help customers maintain peak operational performance. Unified Operations includes AWS Incident Detection and Response and AWS Security Incident Response, described below. For additional protection of critical workloads, FEs can enroll in: • AWS Incident Detection and Response for proactive monitoring and incident management to help customers reduce the potential for failure and accelerate recovery of critical workloads from disruption. • AWS Security Incident Response helps customers prepare for, respond to, and recover from security events through automated security finding monitoring and triage, AI-powered investigation, and containment capabilities. When specialized expertise is required, Security Incident Response gives customers direct 24/7 access to the Security Incident Response engineers, who respond to customers' request within minutes. Both services are included in the Unified Operations support plan. Customers can view or subscribe to AWS Security Bulletins for updates about current vulnerabilities and threats that require attention, including impact assessments and mitigations, and informational bulletins shared for awareness.	Post-Event Summaries (PES)

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
	Although FEs cannot rely solely on AWS notifications to meet DORA reporting obligations and must independently classify incidents, AWS will notify FEs promptly if we become aware of a security incident that impacts them, and we will take steps to address and mitigate any adverse effects, as outlined in the AWS Data Processing Addendum. When an issue that has broad and significant customer impact, AWS provides a public Post-Event Summary (PES) that includes: • Impact scope • Contributing factors • Actions taken to address identified risks Post-Event Summaries remain available for at least 5 years.	
Box 3 Contractual clauses Under Article 30(4) of DORA, supervised entities and cloud service providers must consider using standard contractual clauses developed by public authorities for specific services.	The AWS Customer Agreement contains the terms and conditions that govern customer access to and use of AWS services, and the AWS Service Terms govern customers' use of the services. AWS offers a GDPR-compliant AWS Data Processing Addendum (DPA), to support customers in meeting their GDPR contractual obligations. The AWS DPA is incorporated into the AWS Service Terms and applies automatically to all customers globally who require it to comply with the GDPR whenever customers use AWS services to process personal data, regardless of which data protection laws apply to that processing. AWS offers a Financial Services Addendum (FSA) to financial services customers running regulated workloads. AWS offers a Digital Operational Resilience Act (DORA) FSA which supplements the existing financial services addenda to reflect the contracting requirements of DORA. Eligible customers can contact their AWS Account Manager to request the DORA FSA.	AWS Customer Agreement AWS Service Terms AWS Data Processing Addendum

Summary of expectations	Considerations for FEs that are AWS customers	Additional resources
2.5.3 Internal audits Under Article 8(3) of Commission Delegated Regulation (EU) 2024/1773, supervised entities must not rely solely on CSP-provided third-party audit reports over time. Per Article 6(6) of DORA, internal audit functions should regularly review risks relating to their use of cloud services. Supervised entities may use internal audit functions or appointed third parties.	As mentioned under *2.5.1 Independent monitoring of CSPs*, AWS offers Financial Services Addenda to financial services customers running regulated workloads on AWS. The FSAs include contractual provisions to enable European customers to exercise their audit and access rights with AWS. AWS offers customers options to engage directly with AWS on matters of audit, compliance, and security, and provides tailored mechanisms to directly audit AWS. See more information on: (i) compliance briefings; and (ii) community audits under *2.5.1*. See also the AWS Compliance Programs under *2.1.1* and *2.1.2 Ex ante risk assessment*.	

Next steps

Each organization's cloud adoption journey is unique. FEs need to understand their organization's current state, the desired target state, and the transition required to achieve the target state and manage cloud adoption successfully.

For FEs, the next steps typically include the following:

- Reviewing 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.
- Considering 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.
- Considering using AWS Security Assurance Services to streamline their path to compliance with AWS guidance.
- Contacting their AWS representative to discuss how the AWS Partner Network, AWS Solution Architects, and training instructors can assist with their cloud journey.

Document revisions

Date	Version	DID	Description
May 2026	1.0c	FS1EM0034	First publication