This paper has been archived.

For the latest compliance content, see https://aws.amazon.com/compliance/resources/.

AWS User Guide for U.S. Financial Institutions

October 2018

[Resource Guide]

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. 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.

Contents

Abstract

This document provides information to help U.S. financial institutions (FI) navigate the regulatory implications of using AWS Cloud services and develop a secure, resilient and efficient cloud adoption strategy.

This guide will:

- Provide an overview of regulatory guidance from U.S. banking regulators that FIs typically consider when using AWS.
- Describe the respective roles that the customer and AWS each play in managing and securing the cloud environment
- Provide additional resources that FIs can use to design and architect their AWS environment to be secure and meet regulatory expectations.

The focus of this guide is regulatory guidance from the U.S. banking regulations, including the Board of Governors of the Federal Reserve System (Federal Reserve), the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC). FIs in this guide is meant to refer to those financial institutions subject to oversight by the U.S. banking regulators, as the context requires.

Introduction

In the United States, financial institutions (FI) are permitted to use third-party cloud providers so long as they comply with applicable regulatory requirements. The exact scope and nature of those requirements may be different for each customer based on the types of regulated entities using the cloud as well as the workloads that the customer uses the cloud for.

There are, however, common themes that customers and U.S. banking regulators focus on. In general, the U.S. banking regulators' approach to cloud services focuses on security. Regulators require FIs to perform due diligence on a cloud provider to evaluate its approach to security prior to entering into a relationship and then apply governance and risk management practices to ensure that they use the cloud in a secure way.

This document focuses on typical security-related questions asked by AWS customers when considering their use of AWS services in connection with U.S. banking regulators' guidance.

U.S. Banking Regulators' Guidance for the Use of Cloud

U.S. banking regulators have not issued rules or guidance specifically addressing how FIs should use the cloud. Instead, in the absence of rules tailored to using cloud providers, the U.S. banking regulators typically evaluate an FI's use of the cloud under existing guidance for how FIs should manage "outsourcing" to technology service providers.

An FI's use of a cloud provider such as AWS does not squarely fit the traditional outsourcing model that the U.S. banking regulators' guidance was developed to address. Accordingly, certain aspects of the U.S. banking regulators' existing guidance is not well adapted to the cloud.

In a report on the use of technology in the financial sector, the U.S. Department of the Treasury recognized this misalignment.[1] The Treasury Report summarized the regulatory challenges to cloud adoption:

> "[f]inancial firms face several regulatory challenges related to the adoption of cloud, driven in part by a regulatory regime that has yet to be sufficiently modernized to accommodate cloud and other innovative technologies."

In light of these challenges, the Treasury Report made several recommendations to federal financial regulators to "modernize their requirements and guidance (e.g., vendor oversight) to better provide for appropriate adoption of new technologies such as cloud computing, with the aim of reducing unnecessary barriers to the prudent and informed migration of activities to the cloud."

1 A Financial System that Creates Economic Opportunities, Nonbank Financials, Fintech, and Innovation, U.S. Department of the Treasury, July 2018, available here: https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf (Treasury Report).

As financial regulators and market participants continue to consider the appropriate framework for supervising FIs' use of the cloud, AWS customers can rely on AWS services and information AWS makes available to use AWS in a manner consistent with regulators' current guidance.

This guide focuses on regulatory guidance that AWS customers typically assess when they move to the cloud (together, Outsourcing Guidelines for FIs), including:

- **FFIEC Outsourcing Guidelines for FIs:** The outsourcing portions of the IT Handbooks published by the Federal Financial Institutions Examination Council (FFIEC); and
- **Federal Reserve, OCC and FDIC Guidance:** Guidance from U.S. banking regulators on managing third-party service providers that complements the FFIEC handbooks.

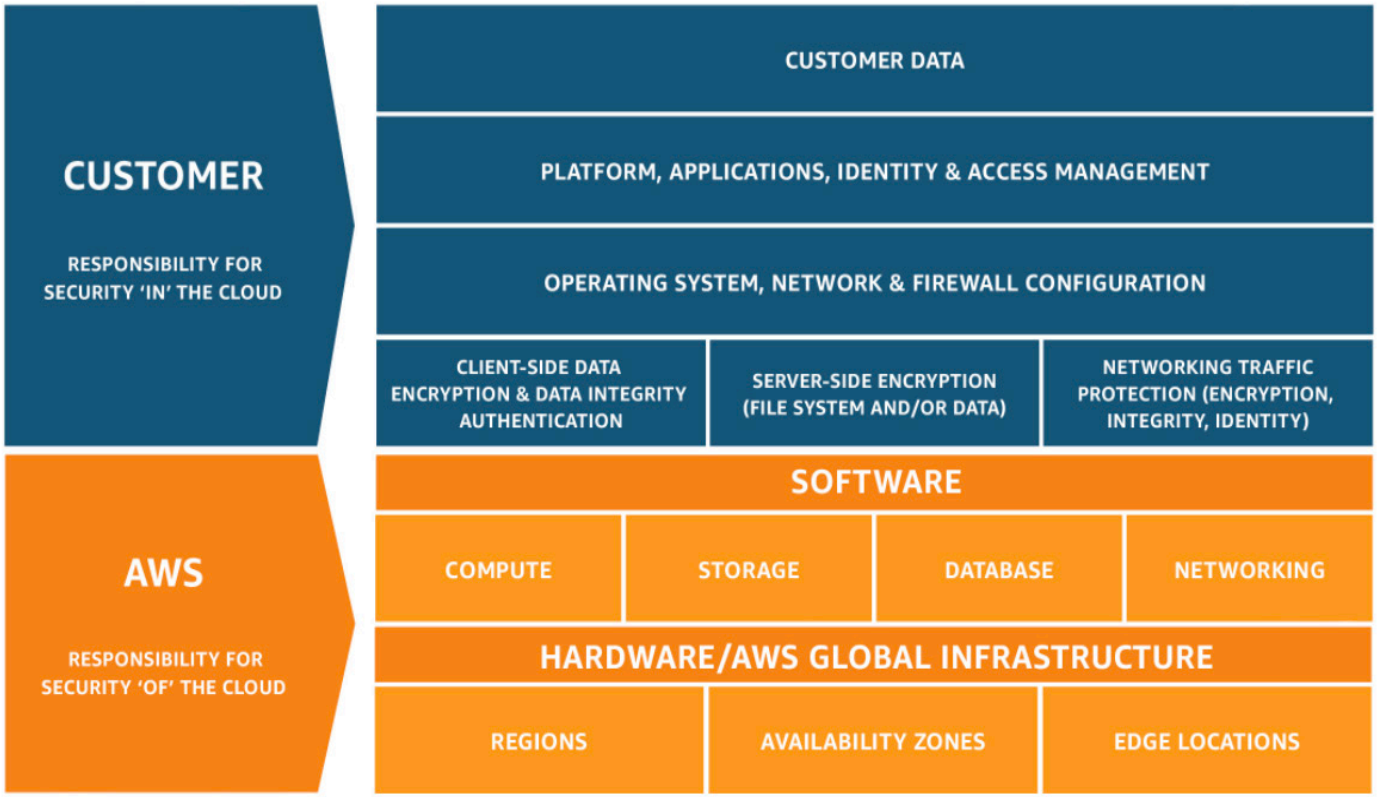
Security, Compliance, and Shared Responsibility

Cloud security is a shared responsibility. Security in the cloud is the responsibility of the customer. What this means is that customers retain control of the security program they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site data center. AWS manages security of the cloud by ensuring that AWS infrastructure complies with global and regional regulatory requirements and best practices.

Understanding the AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the Outsourcing Guidelines for FIs.

To satisfy their regulatory requirements, FIs should ensure that they take steps to secure their AWS environment, i.e., security "in" the cloud, and (2) evaluate the security and resiliency of AWS services and infrastructure, i.e., security of the cloud. AWS has developed a security assurance program to help customers meet these requirements. As discussed below, AWS gives customers access to third-party certifications and audit reports that attest to the AWS security infrastructure and security controls.

Before exploring the specifics of U.S. financial regulation, it is important that FIs understand the AWS Shared Responsibility Model as well as the AWS security assurance program.



AWS Shared Security Responsibility Model

Security in the Cloud

Customers are responsible for their security in the cloud. Much like a traditional data center, the customer is responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as the configuration of the AWS-provided security group firewall. Customers should carefully consider the services they choose, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations.

It is important to note that when using AWS services, customers maintain complete 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 where the content is stored.
- The format and structure of that content and whether it is masked, anonymized, or encrypted.
- How the data is encrypted and where the keys are stored.
- Who has access to that content and how those access rights are granted, managed and revoked.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customers are responsible for the security of the content they put on AWS, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, platforms, databases, or other services.

It is possible to enhance security and/or meet more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection/prevention, and encryption. AWS provides tools and information to assist customers in their efforts to account for and validate that controls are operating effectively in their extended IT environment. More information can be found at the AWS Compliance center.

Security of the Cloud

In order to provide Security of the Cloud, AWS environments are continuously audited, and the infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and verticals. Customers can use these certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications.

The AWS compliance program is based on the following actions:

- **Validate** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment includes policies, processes and control activities that leverage various aspects of Amazon's overall control environment.

  The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of our 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 can implement, and to better assist customers with managing their control environment.

- **Demonstrate** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS. Customers can leverage this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.

- **Monitor** that, through the use of thousands of security control requirements, AWS maintains compliance with global standards and best practices.

AWS Compliance Assurance Programs

AWS has obtained certifications and independent third-party attestations for a variety of industry specific workloads, however the following are of particular importance to FIs:

- **ISO 27001** – ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following 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 which 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** – 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 information security controls implementation guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.
- **ISO 27018** – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public 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** - ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures 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 in a manner where 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 (also known as 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) and/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. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.

- **SOC** – AWS System & 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 established to support operations and compliance. For more information, see the SOC Compliance webpage. There are three types of AWS SOC Reports:
    - **SOC 1**: Provides information about the AWS control environment that may be relevant to a customer's internal controls over financial reporting as well as information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).
    - **SOC 2**: Provides customers and their service users with 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 with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality without disclosing AWS internal information.

By tying together governance-focused, audit-friendly service features with such certifications, attestations and audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment.

For more information about other AWS certifications and attestations, see the AWS Assurance Program webpage. For information about general AWS security controls and service-specific security, see the Amazon Web Services: Overview of Security Processes whitepaper.

Outsourcing Guidelines for FIs

The following sections of the guide address common considerations for FIs that use AWS as they consider the requirements of each of the Outsourcing Guidelines for FIs.

In general, the Outsourcing Guidelines for FIs relate to FIs' risk management programs and how they apply to third-party service providers. It is important to note that U.S. banking regulators typically apply a principles-based approach to evaluate an FI's overall risk-management framework.

Accordingly, it is best practice for FIs to focus not just on specific regulatory requirements but on developing a reliable, secure and efficient system in the cloud and a robust risk management and audit framework for continuous monitoring and evaluation of that system. AWS has developed a comprehensive list of technical whitepapers covering a wide range of topics including security, compliance and in-the-cloud architecture. These whitepapers identify best practices that FIs can follow to maximize the security of their cloud environment and address U.S. banking regulators' evolving risk concerns.

Some key resources for FIs are identified in the "Further Reading" section at the end of this guide.

FFIEC Outsourcing Handbooks

The FFIEC is an inter-agency body that establishes uniform principles, standards and report forms for the federal examination of financial institutions by each of its component agencies.[2] Even though the FFIEC's guidelines are not binding on their own, U.S. banking regulators examine and supervise FIs in accordance with FFIEC guidelines.

The FFIEC's primary guidelines are its "Information Technology Examination Handbook," (IT Handbook) which consists of booklets covering different subject areas in risk management. In a 2012 statement about cloud computing, the FFIEC explained that FIs that use or contemplate using the cloud have to consider the fundamentals of risk and risk management defined in the IT Handbook with a particular emphasis on the aspects of the IT Handbook that deal with managing an outsourcing relationship.[3] This consists of two components of the IT Handbook:

- **Outsourcing Booklet:** U.S. banking regulators examine FIs use of cloud in accordance with the FFIEC Booklet on Outsourcing Technology Services (Outsourcing Booklet). In its 2012 notice, the FFIEC said that it considers the use of cloud computing to be a form of outsourcing and emphasized that FIs should consider the Outsourcing Booklet. The FFIEC identified key areas of focus including due diligence, vendor management, audit, information security, legal, regulatory, and reputational considerations and business continuity planning.
- **BCP Outsourcing Appendix:** The IT Handbook includes a separate booklet specifically on business continuity and includes an appendix specifically dealing with how FIs should think about business continuity in the case of outsourced technology services. This appendix—Business Continuity Planning—Appendix J: Strengthening the Resilience of Outsourced Technology Services (BCP Outsourcing Appendix)—should also be considered by FIs using AWS.

An examination of all aspects of the IT Handbook is beyond the scope of this guide. However, **Appendix A** to this guide provides details on the Outsourcing Booklet and the BCP Outsourcing Appendix and related implementation considerations for AWS customers.

Federal Reserve, OCC and FDIC Guidance

Each of the Federal Reserve, OCC and the FDIC are members of the FFIEC and they examine FIs subject to their respective supervision in accordance with the FFIEC IT Handbooks. The agencies have also each issued their own guidance for FIs about managing third-party relationships, which AWS customers consider when using AWS.

2 The FFIEC's membership includes the Federal Reserve, OCC, FDIC, the National Credit Union Administration, the Consumer Financial Protection Bureau, and the State Liaison Committee.

3 "Outsourced Cloud Computing," July 10, 2012, issued by the FFIEC Information Technology Subcommittee, available at https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf. In this statement, the FFIEC stated that "[f]inancial institutions that contemplate or use a cloud computing model in which all or part of the service is outsourced ("outsourced cloud computing") have to consider the fundamentals of risk and risk management defined in the [IT Handbook], especially the Outsourcing Technology Services Booklet[]."

These agencies' guidance has evolved over many years but some of the key guidance that AWS FI customers focus on are the following (together, the Supplemental Guidance):

- Federal Reserve: Guidance on Managing Outsourcing Risk
- OCC: 2013-29 Risk Management Guidance
- FDIC: Guidance for Managing Third-Party Risk

This guidance is, in all significant respects, consistent with the Outsourcing Booklet, the BCP Outsourcing Booklet, and the considerations set out in **Appendix A**. They do, however, provide greater clarity about the principles that each U.S. banking agency applies when thinking about the risks of outsourcing relationships. Some key considerations from this guidance is discussed below.

Senior Management Responsibilities

One important feature of the Supplemental Guidance is the extent to which the U.S. banking agencies focus on the responsibilities of senior management and an FI's board of directors in developing a comprehensive risk-management process. All three agencies emphasize that the use of service providers does not relieve an FI's board of directors and senior management of their responsibility to ensure that outsourced activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations.

Life-Cycle Risk Management

Another important consideration is the U.S. banking regulators' focus on FIs having an evolving and dynamic risk management system. For example, the OCC's 2013-29 guidance describes third-party risk management as a "life cycle." It explains that "an effective third-party risk management process follows a continuous life cycle for all relationships and incorporates" several different phases from due diligence in selecting a third-party and monitoring the relationship over time.[4] The FFIEC likewise expects FIs to have an effective oversight program that provides the "framework for management to identify, measure, monitor, and control" the risks associated with outsourcing.

FIs can use AWS tools and services to help implement an effective risk management program, monitor its use of AWS and efficiently achieve compliance. For example, AWS Config helps customers continuously monitor and record their AWS resource configurations and automate the evaluation of recorded configurations against desired configurations. Amazon CloudWatch allows customers to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. Customers use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health.

AWS provides up-to-the-minute information on the AWS services that customers use to power their applications via the publicly available Service Health Dashboard. Customers can configure a Personal Health Dashboard to receive a personalized view of the performance and availability of the AWS services underlying their resources

4 The OCC identifies the following phases that a risk-management program for overseeing third-party relationships should address: (1) planning; (2) due diligence and third-party selection; (3) contract negotiation; (4) ongoing monitoring; (5) termination; (6) oversight and accountability; (7) documentation and reporting; and (8) independent review.

and applications. The dashboard displays relevant and timely information to help customers manage events in progress, and it provides proactive notification to help customers plan for scheduled activities. With Personal Health Dashboard, changes in the health of AWS resources automatically trigger alerts, providing event visibility and guidance to help quickly diagnose and resolve issues. Customers can use these insights to react quickly and keep their applications running smoothly.

Business Continuity and Disaster Recovery

U.S. banking regulators expect FIs to evaluate business continuity and develop disaster recovery plans for themselves and to consider business continuity in the context of outsource relationships. FIs that use AWS implement policies and procedures to ensure that their applicable systems have high levels of resiliency and availability.

One example of customers increasing resiliency and availability is using AWS for disaster recovery of their IT systems without incurring the infrastructure expense of a second physical site. With data centers in regions all around the world, AWS provides a set of cloud-based disaster recovery services that enable rapid recovery of customers' IT infrastructure and data. The AWS cloud supports many popular disaster recovery architectures, from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover.

The AWS Cloud infrastructure is built around Regions and Availability Zones ("AZs"). A Region is a physical location in the world where AWS has multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases which are more highly available, fault tolerant and scalable than would be possible from a single data center. The AWS Cloud operates 53 Availability Zones within 18 geographic Regions around the world. For current information on AWS Regions and AZs, see https://aws.amazon.com/about-aws/global-infrastructure/.

AWS customers choose the Region(s) in which their content and servers will be located. This allows customers with certain business continuity and disaster recovery objectives to establish primary and backup environments in a location or locations of their choice.

AWS customers can learn more about disaster recovery on AWS by visiting our website at https://aws.amazon.com/disaster-recovery/. Customers can also read the AWS Disaster Recovery whitepaper to learn about how to architect disaster recovery in the AWS cloud.

Further Reading

Set out below are additional resources to help FIs think about security, compliance and designing a secure and resilient AWS environment.

- AWS Well-Architected Framework: The Well-Architected framework has been developed to help cloud architects build the most secure, high-performing, resilient and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help implement designs that will scale application needs over time. The Well-Architected framework consists of five pillars: Operational Excellence; Security; Reliability; Performance Efficiency; Cost Optimization.
    - AWS has also produced white papers addressing each pillar of the Well-Architected Framework, that are available here: AWS Operational Excellent Pillar Whitepaper; AWS Security Pillar Whitepaper; AWS Reliability Pillar Whitepaper; AWS Performance Efficiency Whitepaper; AWS Cost Optimization Whitepaper.
- **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 shares responsibility model to their regulatory requirements. Customers can access a whitepaper on these principles under a non-disclosure agreement at AWS Artifact.
- **Using AWS For Disaster Recovery:** AWS has released a whitepaper, Using Amazon Web Services for Disaster Recovery, that includes considerations for how customers can architect disaster recovery in the AWS Cloud.
- **NIST Cybersecurity Framework (NIST CSF):** AWS has released a whitepaper, Aligning to the NIST CSF, that 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, i.e., security in the cloud. The whitepaper also provides a third-party auditor letter attesting to the AWS cloud offering's conformance to NIST CSF risk management practices, i.e., security of the cloud. FIs can leverage NIST CSF and AWS's resources to elevate their risk management frameworks to meet evolving U.S. regulatory expectations.

Appendix A—Implementation Considerations

The tables below provides considerations on how AWS FI customers can satisfy the requirements in the Outsourcing Booklet[5] and the BCP Outsourcing Appendix.[6] These tables contains only a non-exhaustive sample of recommendations and associated considerations. This is not legal or compliance advice. Customers should consult with their legal and compliance teams.

FFIEC Outsourcing Booklet		
Objective and Tier	**Outsourcing Booklet Objective**	**AWS Response Information**
Outsourcing Booklet – Objective 1: Determine the Appropriate Scope for the Examination		
Outsourcing Booklet; Appendix A Tier I Objective 1.1	Review past reports for weaknesses involving outsourcing. Consider: • Regulatory reports of examination of the institution and service provider(s); and • Internal and external audit reports of the institution and service provider(s) (if available).	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 the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001, Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards. Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.

5 The table below discusses each of the items in "Appendix A: Examination Procedures" of the Outsourcing Booklet, which sets out the points of focus for federal bank examiners regarding an FI's use of a third-party service provider. The Outsourcing Booklet identifies Tier I objectives and procedures that relate to the FI's implementation of a process for identifying and managing outsourcing risks and Tier II objectives and procedures that provide additional validation and testing techniques as warranted by risk to verify the effectiveness of the FI's process on individual contracts.

6 The BCP Outsourcing Appendix was released by the FFIEC in 2015 as a new part of the FFIEC booklet on business continuity planning. It was added to ensure that the booklet aligns with regulatory guidance on third-party relationship risk management and incorporates emerging risks, such as cyber resilience risk concerns.

Outsourcing Booklet; Appendix A Tier I Objective 1.2	Assess management's response to issues raised since the last examination. Consider: • Resolution of root causes rather than just specific issues; and • Existence of any outstanding issues	Customer responsibility.
Outsourcing Booklet; Appendix A Tier I Objective 1.3	Interview management and review institution information to identify: • Current outsourcing relationships, including cloud computing relationships, and changes to those relationships since the last examination. Also identify any: - Material service provider subcontractors, - Affiliated service providers, - Foreign-based third party providers; • Current transaction volume in each function outsourced; • Any material problems experienced with the service provided; • Service providers with significant financial or control related weaknesses; and • When applicable, whether the primary regulator has been notified of the outsourcing relationship as required by the Bank Service Company Act or Home Owners' Loan Act.	This FFIEC requirement pertains to the customer responsibility to respond to an examiner's review of its outsourcing relationships. To the extent this relates to providing information about an FI's use of AWS, customers can use multiple AWS features to easily and accurately understand and control their IT resources and costs associated with them, and can also quickly obtain an accurate inventory of these resources. • **Account Activity page:** Provides a summarized listing of IT resources by detailing usage of each service by region. • **Amazon Glacier vault inventory:** You can leverage Glacier data inventory to show all IT resources in Glacier. • **AWS CloudHSM:** Virtual and physical control over encryption keys by providing dedicated Hardware Security Modules (HSMs) for key storage. • **AWS Management Console:** Real-time inventory of assets and data by showing all IT resources running in AWS, by service. One-stop-shop view for cost drivers by showing all IT resources running in AWS by service including actual costs and run rate. • **AWS Config:** Discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting. • **AWS Storage Gateway Application Programming Interfaces (APIs):** Inventory assets and data by programming interfaces, tools, and scripts to manage resources. • **Account Activity page:** Anytime view of spending on IT resources by showing resource used by service. • **Amazon EC2 resource tagging:** Conveys association between resource expenditures and business units by applying custom searchable labels to compute resources.

Outsourcing Booklet – Objective 2: Evaluate the Quantity of Risk Present from the Institution's Outsourcing Arrangements		
Outsourcing Booklet; Appendix A Tier I Objective 2.1	Assess the level of risk present in outsourcing arrangements. Consider risks pertaining to: • Functions outsourced; • Service providers, including, where appropriate, unique risks inherent in foreign-based service provider arrangements; and • Technology used.	AWS provides information about its risk and compliance program to enable customers to assess the risk present in using AWS and also to enable customers to incorporate AWS controls into their governance framework. This information can assist customers in documenting a complete control and governance framework with AWS included as an important part of that framework. Consider the following resources: • **Audit Reports and Third-Party Certifications:** AWS provides transparency into the controls in place that prevent unauthorized access to data centers relevant to the Service Organization Controls 1 audit, Payment Card Industry Data Security Standard, ISO 27001 security best practice standard and NIST 800-53 under FedRAMP- which provide an in-depth audit of both the design and operating effectiveness of AWS's defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). Controls are properly designed, tested, and audited by an independent audit firm. • **AWS Trusted Advisor:** AWS customers can use this tool for automated security management assessment that identifies and escalates possible security and permission issues.
Outsourcing Booklet; Appendix A Tier I Objective 2.2	If the institution engages in cloud computing, determine whether: • The cloud computing service is or will be hosted internally or outsourced to a third party provider (hosted externally). • Resources are shared within a single organization or across various clients of the service provider. (Resources can be shared at the network, host, or application level). • The institution has the ability to increase or decrease resources on demand without involving the service provider (on-demand self-service). • Massive scalability in terms of bandwidth or storage is available to the institution. • The institution can rapidly deploy or release resources. • The financial institution pays only for those resources which are actually used (pay-as-you go pricing).	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 it to provide new services that help millions of active customers. AWS is an externally hosted cloud computing service, services can be configured on-demand self-service, are easily scalable, and pay as you go.

Outsourcing Booklet; Appendix A Tier I Objective 2.3; 2.4	If the institution engages in cloud computing, identify: • Objective 2.3: The type(s) of service model that is or will be used; • Objective 2.4: The type of deployment model to be used.	AWS provides standardized services to customers and each customer will have specific AWS configurations. AWS customers can use multiple AWS features to easily and accurately understand and control their IT resources and costs associated with them, and can also quickly obtain an accurate inventory of these resources. See discussion of Tier 1, Objective 1.3, above.
Outsourcing Booklet – Objective 3: Evaluate the Quality of Risk Management		
Outsourcing Booklet; Appendix A Tier I Objective 3.1	Evaluate the outsourcing process for appropriateness given the size and complexity of the institution. The following elements are particularly important: • Institution's evaluation of service providers consistent with scope and criticality of outsourced services; and • Requirements for ongoing monitoring.	AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis. Upon assessment and discovery of risk, Amazon disables accounts that display atypical usage matching the characteristics of bad actors. The AWS Security team extracts all log messages related to system access and provides reports to designated officials. Log analysis is performed to identify events based on defined risk management parameters.

Outsourcing Booklet; Appendix A Tier I Objective 3.2; Tier II Objective A	Tier I Evaluate the requirements definition process. • Ascertain that all stakeholders are involved; the requirements are developed to allow for subsequent use in request for proposals (RFPs), contracts, and monitoring; and actions are required to be documented; and • Ascertain that the requirements definition is sufficiently complete to support the future control efforts of service provider selection, contract preparation, and monitoring. Tier II Review documentation supporting the requirements definition process to ascertain that it appropriately addresses: • Scope and nature; • Standards for controls; • Minimum acceptable service provider characteristics; • Monitoring and reporting; • Transition requirements; • Contract duration, termination, and assignment' and • Contractual protections against liability.	As a customer works through the requirements definition phase, it should understand AWS's commitment to availability. AWS continuously monitors service usage to project infrastructure needs to support availability commitments and requirements. AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely high recovery time and recovery point objectives, as well as service availability of 99.999% and more. If availability and performance are important design considerations for an application, customers should deploy the application across multiple Availability Zones in the same region for fault tolerance and low latency. Some AWS services, such as Amazon S3, are built to leverage all Availability Zones within the region and have a durability objective of 99.999999999%. These services can be used for highly durable storage across Availability Zones and persistent volume (Amazon EBS) snapshots. AWS offers service level agreements for certain AWS services. These may be updated from time to time. The service level agreements we currently offer are located at http://aws.amazon.com/ec2-sla/, http://aws.amazon.com/s3-sla/, http://aws.amazon.com/cloudfront/sla, http://aws.amazon.com/route53/sla, and http://aws.amazon.com/rds/sla.

Outsourcing Booklet; Appendix A Tier I Objective 3.3 Tier II Objective B	Tier I Evaluate the service provider selection process, including the following: • Determine whether due diligence requirements encompass all material aspects of the service provider relationship, such as the provider's financial condition, reputation (e.g., reference checks), controls, key personnel, disaster recovery plans and tests, insurance, communications capabilities and use of subcontractors. Tier II Assess the extent to which the institution reviews the financial stability of the service provider: • Analyzes the service provider's audited financial statements and annual reports; • Assesses the provider's length of operation and market share; • Considers the size of the institution's contract in relation to the size of the company; • Reviews the service provider's level of technological expenditures to ensure ongoing support; and • Assesses the impact of economic, political, or environmental risk on the service provider's financial stability Evaluate whether the institution's due diligence considers the following: • References from current users or user groups about a particular vendor's reputation and performance; • The service provider's experience and ability in the industry; • The service provider's experience and ability in dealing with situations similar to the institution's environment and operations;	AWS can assist customers as they go through an RFP and perform due diligence. Many of the due diligence elements identified by FFIEC refer specifically to the FI's internal process but the below information can help inform the substantive aspects of an FI's assessment of AWS. • **Financial Condition:** The financial statements of Amazon.com Inc include AWS's sales and income, permitting assessment of its financial position and ability to service its debts and/or liabilities. These financial statements are available from the SEC or at Amazon's Investor Relations website. • **Controls:** As discussed above, customers are able to review AWS's control environment by reviewing third-party audit reports, which can be accessed on AWS Artifact. • **Disaster Recovery Plans and Tests:** The AWS Business Continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. This plan has been developed to recover and reconstitute AWS using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach ensures that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and omissions. • **Insurance:** AWS maintains appropriate insurance, including Commercial General Liability insurance with limits of not less than $1,000,000 per occurrence and $5,000,000 general aggregate, and (b) "Crime/Employee Dishonesty" insurance with limits of not less than $500,000 per claim. • **Subcontractors:** AWS uses a number of third-party subcontractors to assist with the provision of its service. However, its subcontractors do not have access to customers' content. In addition, AWS only uses subcontractors that it trusts and it uses appropriate contractual safeguards that it monitors to ensure the required standards are maintained. Details of any subcontractors who have access to customer content, including personal data, are set out on the AWS website, visit the AWS DPA for more information.

	• The quality and effectiveness of any cost/benefit analyses. Determine whether the analysis considered the incremental costs of the additional monitoring, operations responsibilities, and protections that may be required of the financial institution. • The cost for additional system and data conversions or interfaces presented by the various vendors; • Shortcomings in the service provider's expertise that the institution would need to supplement in order to fully mitigate risks; • The service provider's proposed use of third parties, subcontractors, or partners to support the outsourced activities; • The service provider's ability to respond to service disruptions; • Key service provider personnel that would be assigned to support the institution; • The service provider's ability to comply with appropriate federal and state laws. In particular, ensure management has assessed the providers' ability to comply with federal laws (including GLBA and the USA PATRIOT Act); and • Country, state, or locale risk	• **Key Personnel / Training / Expertise:** AWS has implemented formal, documented security awareness and training policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes. The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties. • AWS has developed, documented and disseminated role based security awareness training for personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities. Training includes, but is not limited to the following information (when relevant to the employee's role): - Workforce conduct standards - Candidate background screening procedures - Clear desk policy and procedures - Social engineering, phishing, and malware - Data handling and protection - Compliance commitments - Use of AWS security tools - Security precautions while traveling - How to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel - How to recognize suspicious communications and anomalous behavior in organizational information systems - Practical exercises that reinforce training objectives - ITAR responsibilities

- **AWS Compliance with Federal and State Laws:** AWS formally tracks and monitors its regulatory and contractual agreements and obligations. In order to do so, AWS has performed and maintains the following activities: Identified applicable laws and regulations for each of the jurisdictions in which AWS operates; Documented and maintains all statutory, regulatory and contractual requirements relevant to AWS; Categorized records into types with details of retention periods and type of storage media via the Data Classification Policy; Informed and trains personnel (e.g. employees, contractors, third party users) that must be made aware of compliance policies to protect sensitive AWS information (e.g. intellectual property rights and AWS records) via the Data Handling Policy; Monitors the use of AWS facilities for unauthorized activities with a process in place to enforce appropriate disciplinary action. AWS maintains relationships with outside parties to monitor business and regulatory requirements. Should a new security directive be issued, AWS has documented plans in place to implement that directive with designated timeframes.
    - GLBA Compliance: Most GLBA requirements are controlled by the AWS customer. AWS provides means for customers to protect data, manage permissions and build GLBA-compliant applications on AWS infrastructure. Customers can use AWS Artifact to access AWS's audit reports to gain assurance about AWS's controls.
- **Environmental Risk:** Each AWS data center is evaluated to determine the controls that must be implemented to mitigate, prepare, monitor, and respond to natural disasters or malicious acts that may occur. Controls implemented to address environmental risks can include but are not limited to the following:
    - AWS data centers are equipped with sensors and master shutoff-valves to detect the presence of water. Mechanisms are in place to remove water in order to prevent any additional water damage.
    - Automatic fire detection and suppression equipment has been installed to reduce risk and notify AWS Security Operations Center, and emergency responders in the event of a fire. The fire detection system utilizes smoke detection sensors in all data center environments (e.g., VESDA, point source detection), mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

		• Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at specified levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. This is provided at N+1 and also utilizes free cooling as primary source of cooling when and where it is available based on local environmental conditions. • Availability Zones are physically separated within a metropolitan region and are in different flood plains. • Each Availability Zone is designed as an independent failure zone and automated processes move customer traffic away from the affected area in the case of a failure. • The AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. Power to AWS data centers is provided through local power provider. In the event of disruption, Uninterruptible Power Supply (UPS) units provide back-up power or critical and essential loads in the facility and generators are used to provide back-up power for the entire facility.
Outsourcing Booklet Appendix A Tier I Objective 3.4 Tier II Objective C	Tier I Evaluate the process for entering into a contract with a service provider. Tier II Verify that legal counsel reviewed the contract prior to closing; verify that the contact appropriately addresses certain terms; review service level agreements to ensure they are adequate and measureable; review the institution's process for verifying billing accuracy and monitoring any contract savings through bundling.	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.
Outsourcing Booklet Appendix A Tier I Objective 3.5	If the institution engages in cloud processing, determine that inherent risks have been comprehensively evaluated, control mechanisms have been clearly identified, and that residual risks are at acceptable levels. Ensure that: • Action plans are developed and implemented in instances where residual risk requires further mitigation. • Management updates the risk assessment as necessary.	This FFIEC requirement applies to many aspects of AWS's cloud infrastructure and an FI's use of AWS. The information below can assist FIs develop an action plan and management maintaining a risk assessment of AWS.

	• The types of data in the cloud have been identified (social security numbers, account numbers, IP addresses, etc.) and have established appropriate data classifications based on the financial institution's policies. • The controls are commensurate with the sensitivity and criticality of the data. • The effectiveness of the controls are tested and verified.	AWS has implemented data handling and classification requirements which provide specifications around: • Data encryption • Content in transit and during storage • Access • Retention • Physical controls • Mobile devices • Handling requirements AWS treats all Customer content and associated assets as critical information. AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored. We are vigilant about our customers' security and have implemented sophisticated technical and physical measures against unauthorized access. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.

	• Adequate controls exist over the hypervisor if a virtual machine environment supports the cloud services. • Unless the institution is using private cloud model, determine what controls the institution or service provider established to mitigate the risks of multitenancy.	Different instances running on the same physical machine are isolated from each other via the hypervisor. In addition, the Amazon EC2 firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical random-access memory (RAM) is separated using similar mechanisms. Customer instances have no access to raw disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically erases every block of storage before making it available for use, which protects one customer's data from being unintentionally exposed to another. Customers can further protect their data using traditional file system encryption mechanisms, or, in the case of Amazon Elastic Block Store (EBS) volumes, by enabling AWS-managed disk encryption. Security within Amazon EC2 is provided on multiple levels: the operating system (OS) of the host platform, the virtual instance OS or guest OS, a firewall, and signed API calls. Each of these items builds on the capabilities of the others. This helps prevent data contained within Amazon EC2 from being intercepted by unauthorized systems or users and to provide Amazon EC2 instances themselves security without sacrificing flexibility of configuration.
	• All network traffic is encrypted in the cloud provider's internal network and during transition from the cloud to the institution's network. • All data stored on the service providers systems are being encrypted with unique keys that only authenticated users from this institution can access.	AWS provides multiple options for backup and encryption of customer data. Customers can use Amazon S3 or Amazon Glacier for storage of backup data. All Amazon S3 and Amazon Glacier API endpoints support SSL encryption for data in transit. Amazon Glacier encrypts all data at rest by default. With Amazon S3, customers can choose server-side encryption for objects at rest by letting AWS manage the encryption keys, providing their own keys when they upload an object, or using AWS Key Management Service (AWS KMS) integration for the encryption keys. Alternatively, customers can always encrypt their data before uploading it to AWS. For more information on encryption, see: • AWS Key Management Service Cryptographic Details at https://d1.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf • Encrypting Data at Rest at https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

	• Ensure that the financial institution's business continuity plan addresses contingencies for the cloud computing service. Determine whether the financial institution has an exit strategy and de-conversion plan or strategy for the cloud services.	The AWS Business Continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. This plan has been developed to recover and reconstitute AWS using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach ensures that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and omissions. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.
	• If a financial institution is using the Software as a Service (SaaS) model, determine whether regular backup copies of the data are being made in a format that can be read by the financial institution. (Backup copies made by the service provider may not be readable.)	AWS provides customers with the ability to properly configure and use the AWS service offerings in order to maintain appropriate security, protection, and backup of content, which may include the use of encryption technology to protect content from unauthorized access. Customers maintain full control and responsibility for configuring access to their data. AWS provides APIs for you to configure access control permissions for any of the services you develop or deploy in an AWS environment.

	• Determine whether the cloud service provider has an internal IT audit staff with adequate knowledge and experience or an adequate contractual arrangement with a qualified third-party audit firm.	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 the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001, Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards. Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.
Outsourcing Booklet Appendix A Tier I Objective 3.6 Tier II Objective D	Tier I Evaluate the institution's process for monitoring the risk presented by the service provider relationship. Ascertain that monitoring addresses: • Key service level agreements and contract provisions; • Financial condition of the service provider; • General control environment of the service provider through the receipt and review of appropriate audit and regulatory reports; • Service provider's disaster recovery program and testing; • Information security; • Insurance coverage; • Subcontractor relationships including any changes or control concerns; • Foreign third party relationships; and • Potential changes due to the external environment (i.e., competition and industry trends).	FIs should reference their Enterprise Agreement for the service level agreements and contract provisions. It is the customer's responsibility to monitor its use of AWS. FIs can use AWS tools and services to help implement an effective risk management program, monitor its use of AWS and efficiently achieve compliance. For example, AWS Config helps customers continuously monitor and record their AWS resource configurations and automate the evaluation of recorded configurations against desired configurations. Amazon CloudWatch allows customers to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. Customers use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health For other information relating to this FFIEC requirement, see the responses to Objective 3.3 and 3.5, above.

	Tier II Evaluate the institution's periodic monitoring of the service provider relationship(s), including: • Timeliness of review, given the risk from the relationship; • Changes in the risk due to the function outsourced; • Changing circumstances at the service provider, including financial and control environment changes; • Conformance with the contract, including the service legal agreement; and • Audit reports and other required reporting addressing business continuity, security, and other facets of the outsourcing relationship. Review risk rankings of service providers to ascertain: (1) objectivity; (2) consistency; and (3) compliance with policy. Review actions taken by management when rankings change, to ensure policy conformance when rankings reflect increased risk. • Review any material subcontractor relationships identified by the service provider or in the outsourcing contracts. Ensure: (1) management has reviewed the control environment of all relevant subcontractors for compliance with the institution's requirements definitions and security guidelines; and (2) the institution monitors and documents relevant service provider subcontracting relationships including any changes in the relationships or control concerns.	
Outsourcing Booklet Appendix A Tier I Objective 3.7	Determine whether certain policies and processes have been revised in light of the need for increased controls brought about by the implementation of cloud computing.	Customer responsibility.
Outsourcing Booklet Appendix A Tier I Objective 3.8	Review the policies regarding periodic ranking of service providers by risk for decisions regarding the intensity of monitoring (i.e., risk assessment).	Customer responsibility.

Outsourcing Booklet Appendix A Tier I Objective 3.9	Evaluate the financial institution's use of user groups and other mechanisms to monitor and influence the service provider.	Privileged access to AWS systems are allocated based on least privilege, approved by an authorized individual prior to access provisioning, and assigned a different user ID than used for normal business use. Duties and areas of responsibility (for example, access request and approval, change management request and approval, change development, testing and deployment, etc.) are segregated across different individuals to reduce opportunities for an unauthorized or unintentional modification or misuse of AWS systems. Group or shared accounts are not permitted within the system boundary. Customers retain the ability to manage segregations of duties of their AWS resources.

FFIEC Outsourcing Booklet

BCP Outsourcing Appendix Requirement	AWS Response Information
Third Party Management: FI's risk management program should include outsourced activities that are critical to the FI's ongoing operations. Attention to due diligence, contract management and ongoing monitoring of technology service providers is important to maintaining business resilience.	**Disaster Recovery Plans and Tests**: The AWS Business Continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. This plan has been developed to recover and reconstitute AWS using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach ensures that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and omissions.

Third Party Capacity: FIs should address significant TSP continuity scenarios and service provider alternatives.	AWS continuously monitors service usage to project infrastructure needs to support availability commitments and requirements. AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely high recovery time and recovery point objectives, as well as service availability of 99.999% and more. If availability and performance are important design considerations for an application, customers should deploy the application across multiple Availability Zones in the same region for fault tolerance and low latency. Some AWS services, such as Amazon S3, are built to leverage all Availability Zones within the region and have a durability objective of 99.999999999%. These services can be used for highly durable storage across Availability Zones and persistent volume (Amazon EBS) snapshots. AWS offers service level agreements for certain AWS services. These may be updated from time to time. The service level agreements we currently offer are located at http://aws.amazon.com/ec2-sla/, http://aws.amazon.com/s3-sla/, http://aws.amazon.com/cloudfront/sla, http://aws.amazon.com/route53/sla and http://aws.amazon.com/rds/sla. AWS also offers customers services that can be used to design an exit strategy for services that are internally compatible or externally transferable. For example, AWS Simple Storage Service (S3) and Glacier customers only need to consider how they will export their objects from the services. AWS offers several ways to export customer data, including a large storage appliance service called Snowball.
Testing with Third-Party Service Providers: FIs should address testing scenarios and testing complexity.	AWS tests the Business Continuity plan and its associated procedures at least annually to ensure effectiveness of the plan and the organization readiness to execute the plan. Testing consists of engagement drills that execute on activities that would be performed in an actual outage. AWS documents the results, including lessons learned and any corrective actions that were completed.

Cyber Resilience: FIs should address risks such as malware, insider threats, data or systems destruction and corruption, communications infrastructure disruption, simultaneous attacks on FIs and service providers and incident response.	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics. System activities, including administrator access and approvals, are logged, retained for a defined period of time and protected from unauthorized modifications. AWS requires that the Security and/or affected Service team conduct a post-mortem to determine the cause of incident, as well as to document lessons-learned. AWS employs several automated mechanisms to support incident response and handling requirements, including online reporting and communication tools, a trouble ticketing system, and an incident tracking database.