Coalfire
IT Audit and Compliance

FFIEC Compliance
on
Amazon Web Services

amazon web services

March 2015

Table of Contents

Executive Summary

This Federal Financial Institutions Examination Council (FFIEC) audit and compliance workbook has been designed to guide financial institutions, which are subject to FFIEC audits and compliance responsibilities on the use and security architecture of AWS services. This document is intended for use by AWS financial institution clients, their examiners, and advisors to understand the scope of the AWS services, guidance for implementation, and examination when using AWS services as part of the financial institutions environment for client data.

AWS is audited globally for relevant controls primarily under the Service Organization Controls (SOC) reporting standards and attested to by a Certified Public Account firm. Services may require specific configurations, connectivity and architecture considerations for use within a FFIEC compliant manner. The following document describes the AWS Service Provider controls relevant to FFIEC assessment scope. Additionally, it illustrates the FFIEC compliance responsibilities for AWS and a financial institutions use of AWS.

Description of In-Scope Services

AWS Management Environment is the underlying physical and logical infrastructure, which supports the AWS services including servers, operating systems, hypervisor, and control environment for management and operations of the AWS service.

The AWS Management Environment and the following services were included in the FFIEC controls review:

- Amazon Elastic Compute Cloud (EC2)
- Amazon Virtual Private Cloud (VPC)
- Amazon Elastic Block Storage (EBS)
- Amazon Simple Storage Service (S3)
- Amazon Relational Database Service (RDS)
- Amazon Elastic Load Balancing (ELB)
- Amazon Identity and Access Management (IAM)

For broader descriptions of each service see the AWS Products website .

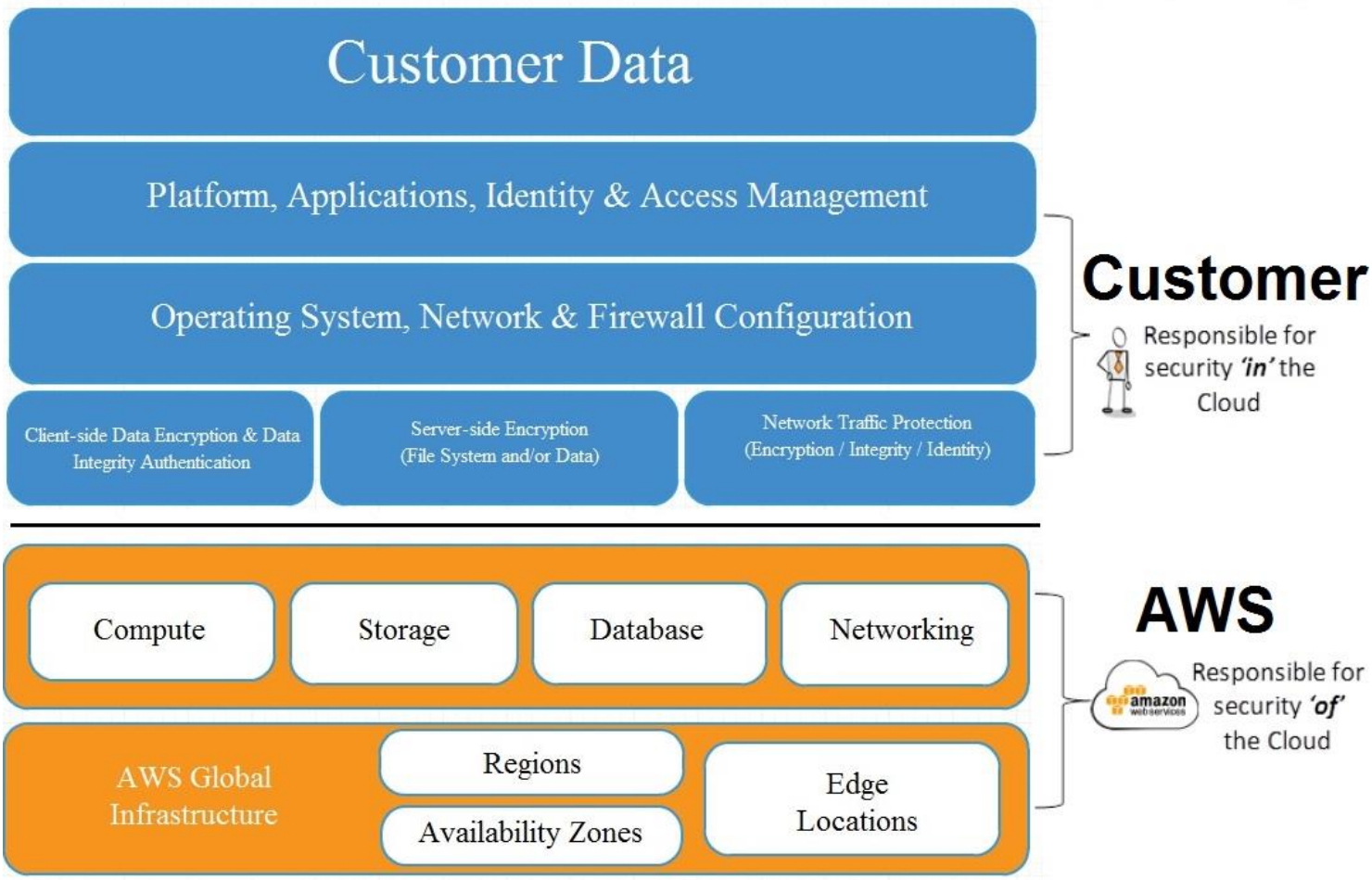
AWS Shared Responsibility Model

To ensure a secure environment, AWS utilizes a shared responsibility model for the operation and management of security controls. This shared model can help relieve a layer of operational burden as both AWS and the client operate and manage components of their information security controls. AWS provides security ***OF*** the cloud, while it is the client's responsibility to develop and maintain security ***IN*** the cloud.

"Security ***OF*** the cloud" pertains to the compliance programs and measures that AWS implements within the cloud infrastructure. AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. "Security ***IN*** the cloud" relates to the client's implementation of security controls associated with their workloads within the AWS infrastructure.

A common question for AWS is: ***"how does leveraging AWS make my security and compliance activities easier?"*** This question can be answered by demonstrating the controls that are met by approaching the AWS Cloud in two distinct ways: first, reviewing compliance of the AWS Infrastructure gives an idea of "compliance ***OF*** the cloud"; and second, the client's review of the compliance standards for the workloads running on top of the AWS infrastructure gives an idea of "compliance ***IN*** the cloud".

The following illustration demonstrates the ***IN*** and ***OF*** responsibilities:



Compliance *OF* the Cloud

Compliance ***OF*** the Cloud refers to how AWS manages the security of the cloud's underlying infrastructure.

How can an organization validate the Security Controls in operation within the AWS Control environment?
AWS certifications and reports are produced by AWS third-party auditors and attest to the design and operating effectiveness of the AWS environment. These include:

i. **SOC 1/ ISAE 3402:** AWS publishes a Service Organization Controls 1 (SOC 1), Type II report. This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report. The SOC 1 report audit attests that the AWS control objectives are appropriately designed and that the controls safeguarding client data are operating effectively.

ii. **SOC 2 - Security:** In addition to the SOC 1 report, AWS publishes a Service Organization Controls 2 (SOC 2), Type II report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security principle set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security based on a defined industry standard and further demonstrates AWS' commitment to protecting client data.

iii. **SOC 3-Security**: AWS publishes a Service Organization Controls 3 (SOC 3) report. The SOC 3 report is a publically available summary of the AWS SOC 2 report and provides the AICPA SysTrust Security Seal. The report includes the external auditor's opinion of the operation of controls (based on the AICPA's Security Trust Principles included in the SOC 2 report), the assertion from AWS management regarding the effectiveness of controls, and an overview of AWS Infrastructure and Services.

iv. **ISO 27001:** AWS is ISO 27001 certified under the International Organization for Standardization (ISO) 27001 standard. ISO 27001 is a widely adopted global security standard that outlines the requirements for information security management systems. It provides a systematic approach to managing company and client information that's based on periodic risk assessments. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and client information.

v. **PCI – Security:** AWS is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS). Clients can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. In February 2013, the PCI Security Standards Council released PCI DSS Cloud Computing Guidelines. These guidelines provide clients who are managing a cardholder data environment with considerations for maintaining PCI DSS controls in the cloud. AWS has incorporated the PCI DSS Cloud Computing Guidelines into the AWS PCI Compliance Package for clients.

In addition to the above-noted reporting, AWS's infrastructure can be used to meet a variety of regulations, standards, and best practices such as the Health Information Portability and Accountability Act (HIPAA), Federal Risk and Authorization Program (FedRAMP) moderate baseline authorization, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), International Traffic and Arms Regulations, the Cloud Security Alliance (CSA) and other requirements, standards, and best practices.

Requesting AWS Compliance Certifications and reports
The applicable AWS compliance certifications and reports can be requested at https://aws.amazon.com/compliance/contact. For more information, the AWS Security Center includes frequently asked questions about compliance and for the AWS Security Whitepaper.

Additional information and resources that describes AWS Compliance environment
AWS has compliance whitepapers providing information to assist AWS clients with integrating AWS into their existing control frameworks and to help design and execute security assessments of an organization's use of AWS.
More information on AWS Compliance certifications, reports, alignment with best practices and standards (such as ISO, PCI-DSS, etc.) can be found at AWS' compliance site.

Compliance *IN* the Cloud

Compliance ***IN*** the Cloud refers to how the client manages the security of their workloads (virtual private clouds, security groups, operating systems, databases, authentication, etc.). Examples are noted below:

Cross-service Controls – Are the responsibility of the client to implement. While each client's use of AWS may vary along with its risk posture and control interpretation, cross service controls will need to be documented within the client's use of the services.

> **Example:** Multi-factor authentication can be used to help secure IAM users within the client environment in-order to meet Access Management, Authentication, and Authorization requirements within a financial

organization.

Service-Specific Controls – Controls specific to a service being used by a client such as the Amazon Simple Storage Service (S3). A client may need to document service specific controls within their use of S3 in-order to meet a specific control objective.

> **Example:** Server Side Encryption (SSE) is enabled for all objects classified per [client] data classification policy as Confidential.

Optimized Network, Operating Systems (OS) and Application Controls – Controls an agency and/or vendor may need to document in-order to meet specific control elements related to the use an approved OS image.

> **Example:** [Client] Server Secure hardening rules or an optimized private Amazon Machine Images (AMI) in order to meet specific controls within Change Management.

Regions, Availability Zones, and Endpoints

Regions, Availability Zones, and endpoints, are components of the AWS secure global infrastructure. Use AWS regions to manage network latency and Contingency Planning (CP) requirements. When you store data in a specific region, it is not replicated outside that region. It is your responsibility to replicate data across regions, if your agencies needs require that. AWS provides information about the country, and, where applicable, the state where each region resides; you are responsible for selecting the region to store data with your network latency requirements in mind. Regions are designed with availability in mind and consist of at least two, often more, Availability Zones.

Availability Zones are designed for fault isolation. They are connected to multiple Internet Service Providers (ISPs) and different power grids. They are interconnected using high-speed links, so applications can rely on Local Area Network (LAN) connectivity for communication between Availability Zones within the same region. Systems can span multiple Availability Zones, and we recommend that you design your systems to survive temporary or prolonged failure of an Availability Zone in the case of a disaster.

Approaches for using this workbook

Examiners

When assessing organizations that use AWS services, it is critical to understand the "Shared Responsibility" model between the client and AWS. The "FFIEC Assessment Guidance for Amazon Web Services" section organizes the requirements into common security program controls and control areas. Each control references the applicable FFIEC requirements, examiner activities, client responsibilities and evidence, and AWS evidence of compliance.

In general, AWS services should be treated like the network infrastructure devices and servers that have been traditionally used by clients to implement services. Policies and processes that apply to devices and servers should also apply when those functions are supplied by AWS services. Controls related to policies or procedures are generally shared or dual controls, as the client needs to extend their governance to their use of AWS services. Similarly, AWS management, either via the AWS Console or Command Line API, should be treated like other privileged administrator access.

AWS services are regularly assessed against applicable standards and requirements. The referenced evidence is validated by third party auditors and made available to clients under appropriate agreements.

Clients

As AWS clients leverage AWS to implement a compliant environment, the following section provides additional information to consider.

- **Authentication and Authorization.** There are two layers of authentication and authorization to consider in the AWS environment: IAM credentials and AWS client controlled credentials.

  IAM provides authentication and authorization for direct access to AWS services by either using local IAM accounts, or integrating access controls with the AWS client's corporate directory such as Active Directory. Regardless of the location of the account, AWS clients create and assign permissions to groups, add additional users, and other activities, which may allow AWS clients to be compliant with many of the access management controls.

  Authentication and authorization of operating systems, and any services or applications running on EC2 or VPC instances are completely under control of the AWS client. AWS clients should design authentication as appropriate for their application environment.

  AWS also provides options to "Federate" authentication. Federated authentication allows for access to the AWS management environment including console and APIs using the organizations Active Directory or other LDAP implementation.

- **Guest Operating System:** the AWS client controls virtual instances in EC2 and VPC. AWS clients have full administrative access and control over accounts, services, and applications.

  - **Choosing an Operating System.** While AWS does provide images that can be used for deployment of host operating systems, AWS clients need to develop and implement system configuration and hardening standards to align with all applicable FFIEC requirements for operating systems. AWS clients own and manage their own instance operating system and the images provided are not intended to represent a compliant platform.

- **Where to Store the Operating System.** AWS provides two places where the base operating system can be stored; the local instance store and EBS. While using a local instance store is an option, this limits the portability of the data and the flexibility of the client's environment. In addition, using a local instance store does not persist beyond the active instance. If that instance is terminated, the instance data is not retrievable. Use of EBS for storage of the operating system, and in fact storage of other on-demand data for the operating system, is a more sustainable model over using local instance storage. EBS also provides functionality to back up to S3 via EBS snapshots.

- **Storage.** AWS provides various options for storage of information including EBS, S3, and RDS, to allow AWS clients to make data easily accessible to their applications or for backup purposes. Storage of sensitive data in the various storage options should be evaluated to as the technology and accessibility of the data to via the Internet to meet FFIEC requirements for restricting direct inbound and outbound access to the systems that contain sensitive data. For example, S3 can be configured to require SSL as well as limit access to pre-defined IP Addresses to limit the accessibility of data from the Internet. Each storage option should be considered and designed to ensure that the use and storage of information is aligned with the relevant requirements.

- **AWS Security Bulletins.** AWS has processes in place to identify and remediate security vulnerabilities that exist within the platform and applications that they manage. As a result of the continuous security improvements that are made within the environment, AWS Security Bulletins are published and communicated to AWS clients regarding security related information that may affect the services and provide guidance to mitigate the risks identified. AWS clients should include the review of these bulletins in their vulnerability management programs and ensure that any applicable recommendations are applied to the affected services.

- **Encryption.** AWS clients retain the responsibility for transport and storage encryption of sensitive data for their environment.

- **Backup of Data.** AWS clients can architect redundant servers for resiliency and rely on S3 replication (which is stored in multiple redundant locations, by default). Any other backup options that AWS clients may implement are at their sole discretion to configure and manage outside of the AWS services offered and validated. AWS does not backup client data to removable media.

- **Using VPC.** VPC is a secure bridge between a company's existing IT infrastructure and the AWS cloud. This service enables enterprises to connect their existing infrastructure to a set of isolated AWS compute resources via a Virtual Private Network (VPN) connection, and to extend their existing management capabilities such as security services, firewalls, and intrusion detection systems to include their AWS resources. VPC can also be configured to create a public-facing subnet for a company's webservers that has access to the Internet. Currently VPC integrates with EC2 and RDS, and may integrate with other AWS services in the future. This service can be leveraged as required to create a compliant environment and reduce public access to specific segments of the AWS client's network as well as secure channels to AWS data storage options.

- **Audit logging.** AWS provides the ability for clients to log all AWS management activities using CloudTrail. When clients enable CloudTrail, all AWS API calls, both from the Console and CLI, are logged. Logs are provided via an S3 bucket so that clients can configure appropriate permissions and retention.

- **Forensic Investigations.** AWS will cooperate with forensic investigations as required by law. AWS will work with clients and designated forensic investigators as required for forensic investigations.

- **Use of Other AWS Services.** At this time EC2, VPC, S3, EBS, RDS, ELB, and IAM, are all covered under this guidance. Other services are not listed explicitly in scope, as they were not evaluated by AWS for FFIEC requirements.

AWS Provided Evidence

AWS services are regularly assessed against applicable standards and requirements. In an attempt to support a variety of industries including federal agencies, retailers, international organizations, health care providers and financial institutions, AWS elects to have a variety of assessments performed against the services and infrastructure. For a complete list and information on assessment performed by third parties please refer to AWS Compliance web site.

The "FFIEC Assessment Guidance for Amazon Web Services" section of this document provides the appropriate references to some of the primary audit documents that can be used to evidence AWS controls, which align with the FFIEC guidance.

Amazon Web Services: http://aws.amazon.com/compliance
Contact: http://aws.amazon.com/compliance/contact/

Coalfire: www.coalfire.com
Phone: 877-224-8077
Email: info@coalfire.com

FFIEC Assessment Guidance for Amazon Web Services

AWS compliance program assures that AWS services are regularly audited against applicable standards. Some control statements may be satisfied by the client's use of AWS (for instance Physical access to sensitive data). However, most controls have either shared responsibilities between the AWS client and AWS, or are entirely the client's responsibility. This section describes the responsibilities that AWS assumes for the services offered and the client's responsibilities when utilizing the in-scope AWS services.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
IT Security Program and Policy						
SP-1	IT Security Program and Policy	Develop, document, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to the size and complexity of the organization, the nature and scope of your activities, contains the objectives of the program, assigns responsibility for implementation, and provides methods for compliance and enforcement. Does the board of directors or appropriate senior management approve this program? Does it include a statement of intent from management that it supports the objectives and principles of the information security program?	FFIEC IS Booklet (2006) Appendix A: Objective 4, Objective 7 p. A4-A5, p. A7 FFIEC MGT Booklet (2004) Appendix A: Objective 4, Objective 6 p. A5-A6, p. A7-A8	The examiner should review the security policy and program documentations related to the use of AWS services administration and security roles definitions The examiner should verify if the AWS services are appropriately addressed within the information security program. Additionally, the examiner should verify there is appropriate approval for the use of AWS. **Examiner should request & review:** 1. Information Security program charter 2. Information Security Policies 3. AWS administration & security role definition	Review your organization's information security, privacy, and data classification policies to determine which policies apply to the AWS service environment. AWS client are responsible for the security of the following assets groups: • Amazon Machine Images (AMIs) • Operating systems • Applications • Data in transit • Data at rest • Data stores • Credentials IT security policies should be documented based on your use of AWS service and how they conform align your existing information security policies.	AWS has implemented a formal information security program designed to protect the confidentiality, integrity, and availability of clients' systems and data. AWS maintains the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy. **Reference:** ISO/IEC 27001:2005 Control: A.5.1.1 Service Organization Controls (SOC) 2 – Section III Area A PCI DSS v3.0 Requirement 12
SP-2	IT Security Program and Policy	Is there a designated employee or employees to coordinate your information security program	FFIEC IS Booklet (2006) Appendix A: Objective 7	The examiner should determine if the organization has assigns an employee to coordinate the information security program. **Examiner should request & review:**	Organization should designate an employee for security responsibility and the designation should be extend to use of AWS services	An AWS Chief Information Security Officer (CISO) exists and is responsible for coordinating, developing, implementing, and maintaining an organization-wide information security program. **Reference:**

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
				1. Documentation which defines employees' Information Security authority and; 2. The authority extends to the use and security configuration of AWS services		ISO/IEC 27001:2005 Control: A.6.1.2 SOC 2 – Section III Area C PCI DSS v3.0 Requirement 12
SP-3	IT Security Program and Policy	Is the security program periodically updated to reflect changes in the organization's operations and systems, as well as changes in the threats or risks to the organization's client information?	FFIEC IS Booklet (2006) Appendix A: Objective 4.2 p. A5	The examiner should verify the client security program is periodically updated to reflect changes in AWS services subscribed by the organization. **Examiner should request & review:** 1. Changes to AWS operations and systems, as well as changes in the threats or risks related to client uses of AWS services 2. Risk Assessment and verify risk and threats related to the use of AWS services have been identified and risk treatment measures are in-place **Reference**: AWS Security Bulletins	Re-assess and review your organization's security, privacy, and data classification policies to determine which policies apply to the AWS service environment. Identify and document threats and risk associated with your use of AWS services within annual risk assessment and outline risk treatments and/or mitigations.	AWS management re-evaluates the security program at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks. **Reference:** NIST SP 800-53 rev.3 FedRAMP Control: CA-2 (2) SOC 2 – Section III Area A PCI DSS v3.0 Requirement 12
SP-4	IT Security Program and Policy	Are the roles and responsibilities for the Board of Directors (BOD), managers and employees clearly defined in the information security policy? Responsible parties should be capable of assisting security personnel in the implementation of the organizational security program. Some of the key roles and responsibilities are: - Information Security Officer (ISO) - IT steering committee - Incident response team - Business Continuity team	FFIEC IS Booklet (2006) Appendix A: Objective 7 p. A7 FFIEC MGT Booklet (2004) Appendix A: Objective 2, Objective 4 p. A2-A3, A5-A6 FFIEC OPS Booklet (2004) Appendix A: Objective 2 p. A2	The examiner should verify that the roles and responsibilities for the Board of Directors (BOD), managers and employees are clearly defined in the information security policy and responsible parties are capable of assisting security personnel in the implementation of the organizational security program relate to the use and configuration of AWS services. **Examiner should request & review:** 1. If AWS service responsibility has been defined and documented within the following roles: - Information Security Officer (ISO) - IT steering committee - Incident response team	Document internal roles and responsibilities related to the Administration, Security, Resiliency and Management oversight of AWS services. Define AWS service responsibility for the following roles or similar roles based on your organizational framework: - Information Security Officer (ISO) - IT steering committee - Incident response team - Business Continuity Team	An AWS Chief Information Security Officer (CISO) exists and is responsible for coordinating, developing, implementing, and maintaining an organization-wide information security program. **Reference:** ISO/IEC 27001:2005 Control: A.5.1.3 SOC 2 – Section III, 'Relevant Aspects of Internal Controls' PCI DSS v3.0 Requirement 12

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
				- Business Continuity Team		
SP-5	IT Security Program and Policy	Does the institution have a set of IT security policies? Does it take into consideration the institution size and complexity? Some of the policies needed are: - Acceptable use - Access control - Change control - Roles and responsibilities - Personnel security - Physical security - Systems development/acquisition and maintenance - Vendor management and outsourcing - Encryption - Information security operations - Back-up - Media disposition, transport and handling - Security review and Assessment - Incident response - Firewall policy - Assessment and logging	FFIEC IS Booklet (2006) Appendix A: Objective 2 p. A2-A3 FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC MGT Booklet (2004) Appendix A: Objective 3, Objective 6 p. A3-A5, A7-A8	The examiner should verify the institution has a set of security policies and the use of AWS service is documented based on the organizational size and complexity of the services deployed. **Examiner should request & review:** 1. Acceptable use, Access Control, Change Management, Vendor Management standards and procedures 2. AWS Access Controls Configurations samples 3. AWS Change Management sample of a change requests	A formal IT security program should be developed for managing client information. The institution must have a set of IT security policies that take into consideration the institution size and complexity. The policies should include use and management of AWS services.	The ISMS program along with the Security Policy and related procedures are reviewed at planned intervals and action plans are identified to address areas with noted issues. **Reference:** ISO/IEC 27001:2005 Control: A.5.1.2 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
SP-6	IT Security Program and Policy	Is there a documented policy and guidelines for the appropriate disclosure of client information? Staff should be trained on such policies.	FFIEC IS Booklet (2006) Appendix A: Objective 6 p. A6-A7 Standards for Safety and Soundness: Supplement A to Appendix B	The examiner should verify that there is a documented policy and guidelines for the appropriate disclosure of client information within internal systems as well as external service use such as AWS. Examiner should verify staff is trained on this policy. **Examiner should request & review:** 1. Data Classification policy/procedures 2. Incident Response processes	Organization should establish a policy and guidelines for the appropriate disclosure of client information within both internal and external services, which document the appropriate data classification standards for information with the AWS service environments. Additionally ensure staff is trained on the policy procedure and incident report process if information is inappropriately handled.	AWS employees are required to review and sign-off on an employment contract, which acknowledges their responsibilities to overall Company standards and information security, which includes processes for discloser of client information. Confidentiality agreements, which include information protection requirements, are reviewed and signed-off by all Amazon employees.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
			12 CFR § 364 (2005)	3. Staff training related to data management and disclosure		**Reference**: ISO/IEC 27001:2005 Control: A.6.1.5 & A.7.1.3 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
SP-7	IT Security Program and Policy	Does Management and the BOD review and approve on a periodic basis: - Updated information security program - Updated policies	FFIEC IS Booklet (2006) Appendix A: Objective 4.2 p. A5 FFIEC MGT Booklet (2004) Appendix A: Objective 3, Objective 5 p. A3-A5, A6-A7	The examiner should verify that Management and review and approve on a periodic basis updates to the information security program and policies to include changes in the use and configuration of the AWS services. **Examiner should request & review:** 1. Vendor management reports related to the use of AWS service 2. Validated if all the services in use within the organization are documented within the information security program and policies	The organization should establish a schedule for updating the information security program and policies to include the uses of AWS services within the organization and any Management review process necessary to include BOD as appropriate.	The ISMS program along with the Security Policy and related procedures are reviewed at planned intervals and action plans are identified to address areas with noted issues. **Reference**: ISO/IEC 27001:2005 Control: A.5.1.2 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
SP-8	IT Security Program and Policy	Are security Policies enforced using either security tools or sanctions for non-compliance? Are Policies and sanctions communicated clearly too all employees?	FFIEC IS Booklet (2006) Appendix A: Objective 4.2 p. A5 FFIEC IS Booklet (2006) Appendix A: Tier II: F p. A16	The examiner should verify that security policies are enforced using either security tools or sanctions for non-compliance. **Examiner should request & review:** 1. The organization's uses of Security Information and Event Management (SIEM) systems to determine if alarming is coming from the AWS environments is being identified and addressed in a timely manner and the response is in alignment with organizational policies and procedures 2. Review the use of any AWS reporting tools such as: a. Amazon CloudWatch b. AWS Trusted Advisor	The organization should integrate AWS services into their Security Information and Event Management (SIEM) tools and ensure their policies, procedures for non-compliance and sanctions within the organization are clearly communicated. Additionally, organization should evaluated and use AWS tools and service to monitor security processes and configurations Tool examples: 1. Amazon CloudWatch 2. AWS Trusted Advisor	AWS employs a formal sanctions process for personnel violating information security policies and procedures through the use of development lists in Amazon's Human Resource Management System (HRMS). **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: PS-8 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
Information Security Oversight						
OV-1	Information Security Oversight	Has the BOD/Senior Management clearly communicated to IS Management its expectations and requirements in a written form on how the following will be conducted: - Central oversight and coordination - Role and responsibilities of the organization's security program - Risk measurement - Monitoring and testing - Reporting functions of the organization's security process to test operating effectiveness - Security reports on alerts and exceptions - Residual risk acceptable for the organization	FFIEC IS Booklet (2006) Appendix A: Objective 4.2 p. A5 FFIEC MGT Booklet (2004) Appendix A: Objective 3, Objective 5 p. A3-A5, A6-A7 FFIEC OPS Booklet (2004) Appendix A: Objective 2 p. A2-A3 FFIEC AUD Booklet (2012) Appendix A: Objective 2 p. A2-A3	Examiner review if roles and responsibilities have been defined related to the central oversight to the use of AWS services Determine whether AWS serviced has been integrated into risk assessment processes. If yes, evaluate the significance of the AWS deployment to the organization's overall risk profile and risk tolerance. **Examiner should request and review:** 1. Software Development Lifecycle (SDLC) process related to AWS services. 2. AWS service testing and monitoring processes 3. Risk Assessment and risk treatment plans related to AWS services	Review your organization's security, policies and procedures to determine which policies elements (e.g. Roles & Responsibilities, Risk Management, and Monitoring & Reporting) apply to the AWS service environment. Organization should ensure their use of AWS services is included in the: 1. SDLC processes 2. Service testing & Monitoring 3. Risk Assessment & treatment plans. 4. Security Reporting AWS Security Bulletins	AWS management has developed a strategic business plan, which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: RA-1 SOC 2 – Section III PCI DSS v3.0 Requirement 12
OV-2	Information Security Oversight	Does the organization perform an annual independent assessment to test the operating effectiveness of internal controls?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC AUD Booklet (2012) Appendix A: Objective 10 p. A6-A7	The examiner should verify annual third party assessment tests, which test the operating effectiveness of internal controls to include the integration of AWS services in use by the organization. **Examiner should request and review** 1. External report of controls for the organization **Example Reports:** *2.* Service Organization Control (SOC) 1 *3.* Service Organization Control (SOC) 2 *4.* Payment Card Industry (PCI) Attestation of Compliance	Clients are responsible for the security of anything their organization puts on their AWS assets or connect to their AWS assets, such as the guest operating system and applications on their virtual machine instance, the data and objects in their S3 buckets or RDS database, etc. Clients should work with their external assessors to help them understand their use can configuration of AWS services	AWS provides a secure global infrastructure and services for which AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. The applicable AWS compliance certifications and reports can be requested see link: AWS Compliance Requests **Reference**: SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
OV-3	Information Security Oversight	Do the BOD and Senior Management receive periodic reports to verify enforcement of the security program and effectiveness of controls?	FFIEC MGT Booklet (2004) Appendix A: Objective 3, Objective 5 p. A3-A5, A6-A7 FFIEC OPS Booklet (2004) Appendix A: Objective 3 p. A3	The examiner should check if the Board of Directors and senior management receive periodic reports on reports on controls to verify enforcement of the security program and effectiveness of controls related to internal and AWS services. **Examiner should request and review** 1. Senior Staff Information Security briefings, 2. BOD meeting agendas and meeting notes 3. Report of Controls	The organization should ensure the information security program conducts re-occurring security briefings with internal management the BOD is briefed on reports of controls for both internal systems as well as AWS services.	The AWS Compliance Managers communicate the various reports of controls on a reoccurring basis based on the annual audit schedules of the various third-party reviews. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CA-2 (1) SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
OV-4	Information Security Oversight	Does Senior Management take appropriate and timely action on IT assessment findings and recommendations, and whether assessment or management reports the action to the BOD or its assessment committee?	FFIEC IS Booklet (2006) Appendix A: Objective 7 p. A7 FFIEC MGT Booklet (2004) Appendix A: Objective 5 p. A6-A7	The examiner should review the assessment findings for internal and AWS services and determine if appropriate remediation activities have been created, tracked and completed to mitigate the risks. **Examiner should request and review** 1. Risk Treatment Plans with timelines and milestones 2. Risk Treatment meeting notes with Senior Management 3. Findings remediation documentation	The organization should have a program and process to assess the risk of the findings from the internal assessment and document the remediation activities and reporting process to their management.	AWS maintains a Plan of Action and Milestones (POA&M) program for the systems with identified planned or correct action needed due to differences from FISMA standards and the AWS service deployment noted during the annual assessments of security controls. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CA-5 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
Risk Assessment						
RA-1	Risk Assessment	Has a comprehensive risk assessment that requires a thorough review of all critical business processes been conducted by a multi-disciplinary management team using a well-accepted methodology? Does it take into consideration the locations, systems, and methods for storing, processing, transmitting, and disposing of client information and identifies	FFIEC IS Booklet (2006) Appendix A: Objective 3 p. A3-A4 FFIEC OPS Booklet (2004) Appendix A: Objective 3, Objective 5 p. A3, p. A4-A5	The examiner should verify the client has integrating the use of AWS services into the organizational risk assessment and has identified critical business processes which are hosted within AWS. Additionally, evaluate the significance of the AWS-deployment to the organization's overall risk profile and risk tolerance. **Examiner should request and review**:	Incorporate use of AWS into risk assessment. Conduct and/or incorporate AWS service elements into your organizational risk assessment processes. Key risks could include: • Identify the business risk associated with your use of AWS and identify business owners and key stakeholders. • Verify that the business risks are aligned, rated, or	An annual risk assessment, which covers all AWS regions and businesses, is conducted by the AWS Compliance team and reviewed by AWS Senior Management (including the AWS CISO, VP of Finance, and VPs of service operations). This is in addition to the Security Assessment conducted by an independent auditor. The purpose of the risk assessment is to check the company's compliance

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		reasonably foreseeable internal and external threats to client information and/or information systems and a likelihood and impact analysis? Is the security program based on the risk assessment? Is the risk assessment well documented, reviewed and updated as required upon key system or process changes?		1. Latest risk assessment to determine if AWS services have been included in the scope 2. Risk Treatment plans to determine if identified remediation is following a defied timeline with milestone process to correct the identified deficiencies	classified within your use of AWS services and your organizational security criteria for protecting confidentiality, integrity, and availability. • Review previous audits related to AWS services (SOC, PCI, NIST 800-53 related audits, etc.). • Determine if the risks identified previously have been appropriately addressed. • Evaluate the overall risk factor for performing your AWS review.	with security policies and standards, to identify threats and vulnerabilities of AWS (which includes AWS), to assign the threats and vulnerabilities a risk rating, to formally document the assessment, and to create a risk treatment plan for addressing issues. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: RA-1 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
RA-2	Risk Assessment	Has a system characterization been done as part of the risk assessment to identify and rank information assets (e.g. data systems, physical locations)?	FFIEC IS Booklet (2006) Appendix A: Objective 3 p. A3-A4	The examiner should check if system characterization been documented for AWS services as part of the risk assessment to identify and rank information assets (e.g. applications data systems, etc.). **Examiner should request and review:** 1. Latest risk assessment to determine if AWS services have characterized and risk ranked	Client should Identify the business risk associated with their use of AWS and identify business owners and key stakeholders in an effort to evaluate the overall risk factor for the use of AWS services.	Security categorization is an organization-wide activity conducted by the AWS Compliance team in conjunction with AWS Service Owners during service on boarding and within the annual risk assessments. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: RA-2 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
RA-3	Risk Assessment	Has the risk assessment taken into consideration both institution and client privacy protection?	FFIEC IS Booklet (2006) Appendix A: Objective 3 p. A3-A4	The examiner should verify the risk assessment includes consideration for the use of AWS service as they relate to institutional and client privacy protection. Examiner should request and review: 1. Latest risk assessment to determine if a privacy impact assessment has been completed which includes considerations for the use of AWS services	Clients would be responsible for managing privacy matters regarding the handling and storage of their data as well as conducting risk assessments on their use of AWS services as it relates to privacy protections.	AWS completes annual Privacy Impact Assessment (PIA) as part of US Federal compliance efforts. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: PL-5 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12 For more information see: AWS privacy notices

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
RA-4	Risk Assessment	Does the risk assessment take into consideration third party service providers and risks due to outsourcing relationships?	FFIEC IS Booklet (2006) Appendix A: Objective 3, Objective 5 p. A3-A4, A5-A6	The examiner should check that the risk assessment take into consideration third party service providers and risks due to outsourcing relationships, including AWS. **Examiner should request and review:** 1. Third party vendor management policies & procedures 2. Third party pre-contracting risk assessments and/or security reviews	Organizations should develop a process for managing risk assessment process related to third party service providers and document risks associated with outsourcing relationships to include AWS service use.	The AWS Secure Software Development Process outlines the security reviews process for External Party reviews and the Third Party Software Review Process. AWS maintains a list approved provider and unapproved third party providers. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SA-2 SOC 2 – Section III PCI DSS v3.0 Requirement 12
RA-5	Risk Assessment	Does the BOD or designated oversight committee periodically reviews the risk assessment process?	FFIEC IS Booklet (2006) Appendix A: Objective 3 p. A3-A4 FFIEC MGT Booklet (2004) Appendix A: Objective 5 p. A6-A7	The examiner should check that the BOD or designated oversight committee periodically reviews the risk assessment process. **Examiner should request and review**: 1. Periodic BOD agendas, meeting minutes and briefings delivered related to risk assessments and treatment activities	Organizations should ensure their risk assessment process includes oversight definitions (e.g. Management and BOD) reviews and approvals which includes he use of AWS services used within the organization.	An annual risk assessment, which covers all AWS regions and businesses, is conducted by the AWS Compliance team and reviewed by AWS Senior Management (including the AWS CISO, VP of Finance, and VPs of service operations). **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: RA-1 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
Incident Response						
IR-1	Incident Response	Is there a formal and well-documented incident response plan and policy, which includes appropriate reporting to regulatory and enforcement agencies? The incident response plan should include detailed incident response procedures in place that outlines the processes for incident handling This includes: - Roles and responsibilities - Initial response - Containment - Restoration of systems	FFIEC IS Booklet (2006) Appendix A: Objective 6 p. A6-A7 FFIEC OPS Booklet (2004) Appendix A: Objective 10 p. A8-A9	The examiner should verify if the incident response plan and policy includes appropriate AWS reporting processes as well as communication procedures between the organization and AWS. **Examiner should request and review**: 1. Incident Response policies, plans and procedure 2. Incident Response plan coordination documentation and commitments between the organization and AWS	The AWS shared responsibility model requires you to monitor and manage your environment at the operating system and higher layers. Organization should adapt your existing incident response policies, processes, tools, and methodologies based on your use AWS services.	AWS has implemented a formal, documented incident response policy called “AWS Incident Response Policy,” which is updated and reviewed annually. The Incident Response Policy is disseminated via the internal Amazon portal to all employees and contractors. The AWS Compliance team, with approval by the AWS Chief Information Security Officer, reviews this policy annually. This policy addresses purpose, scope, roles, responsibilities, and management commitment.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		- Reporting				**Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IR-1 SOC 2 – Appendix 1, Security Policy Criteria 1.2 Mapping PCI DSS v3.0 Requirement 12
IR-2	Incident Response	Are there adequate incident monitoring tools such as assessment logging, Network and Host based IDS deployed?	FFIEC IS Booklet (2006) Appendix A: Objective 6 p. A6-A7	The examiner should verify the organization has adequately updated and leveraged their existing incident monitoring tools as well as AWS available tools to monitor the use of AWS services. **Examiner should request and review** 1. The use of internal incident response and monitoring tools 2. Tools used within the AWS service environment **Examples include:** • AWS CloudWatch • EC2 Describe API • Amazon Simple Notification Service • AWS Health Dashboard • AWS CloudTrail logs • AWS Config	Clients should incorporate AWS services and tools into their incident response plan. **Examples include:** • AWS CloudWatch • EC2 Describe API • Amazon Simple Notification Service • AWS Health Dashboard • AWS CloudTrail logs • AWS Config These AWS service can be useful for monitoring AWS services.	The Amazon Incident Management team employs industry standard diagnostic procedures to drive resolution during Business impacting events. Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and resolution. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IR-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 12
IR-3	Incident Response	Are there defined thresholds to escalate events to incidents?	FFIEC IS Booklet (2006) Appendix A: Objective 6 p. A6-A7 FFIEC OPS Booklet (2004) Appendix A: Objective 10 p. A8-A9	The examiner should verify the organizational use of AWS services aligns and can support their internally defined thresholds. **Examiner should request and review** 1. Documentation, which designates thresholds and escalation procedures 2. Compare the documented thresholds with the internal tools as well as the AWS tools in-place in an effort to verify they support and align to the stated values defined	Client should configure AWS monitoring services to comply with their internally defined thresholds and escalations processes.	AWS has in place the various processes required to handle security incidents such as preparation activities, detection and analysis capabilities, as well as containment, eradication, and recovery procedures. AWS responds to multiple events across various AWS services; therefore there are no specific thresholds defined within AWS. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IR-4 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 12

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
IR-4	Incident Response	Does the Incident Response Plan undergo an annual review and changes made as needed?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC OPS Booklet (2004) Appendix A: Objective 3 p. A3	The examiner should check that the Incident Response Plan undergoes an annual review and changes related to AWS are made as needed. **Examiner should request and review** 1. Documentation related incident response plan reviews	Organizations should define an annual incident response process review which includes lessons learn from exercises, real world incidents and changes to the services environments to include the AWS services in use.	AWS has implemented a formal, documented incident response policy called "AWS Incident Response Policy," which is updated and reviewed annually. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IR-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 12
IR-5	Incident Response	Does the Incident Response Plan require the notification of clients in the event that client information is improperly disclosed?	FFIEC IS Booklet (2006) Appendix A: Objective 6 p. A6-A7	The examiner should check if the incident response plan has client impact notification procedures. **Examiner should request and review** 1. Documentation related to escalation and notification procedures	Organization should ensure documentation is in place related to escalation and client notification in the event of information discloser.	AWS will report incidents affecting clients in accordance with the AWS Incident Response Plan. All investigations, which involve AWS systems, hosts, logs, and records, are conducted by the AWS Security team **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IR-6 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 12
Personnel Controls						
PE-1	Personnel Controls	Is all IT operations staff in sensitive or trusted positions with access to client information subject to a comprehensive screening process during hiring, including background checks?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: F p. A16 FFIEC OPS Booklet (2004) Appendix A: Objective 5 p. A4-A5	The examiner should verify the organizations personnel security (PS) program includes references to the AWS services support personnel designations. **Examiner should request and review** 1. The organizational background screening processes 2. Policy and procedures related to trusted position designations	Organizations should ensure their internal screening process aligns and defines trusted positions and aligns to access level assignments for both internal and external services such as AWS.	All AWS personnel supporting systems and devices within the AWS are classified as high-risk designations within AWS parent organization, Amazon.com. These personnel are considered as having positions having access to sensitive AWS trade secrets, confidential or proprietary information or other valuable company assets. An extensive background check is performed on all AWS personnel as part of the pre-employment process. **Reference**:

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
						NIST SP 800-53 rev.3 FedRAMP Control: PS-1 SOC 2 – Security Procedures Criteria 3.11 description PCI DSS v3.0 Requirement 12
PE-2	Personnel Controls	Is there adequate segregation of duties, IT personnel performing data security activities are independent from systems and programming, computer operations, data input/output, and assessment activities and where feasible, management should implement segregation and rotation of duties among IT staff to prevent fraud and dishonesty?	FFIEC IS Booklet (2006) Appendix A: Objective 7 p. A7 FFIEC MGT Booklet (2004) Appendix A: Objective 2 p. A2-A3 FFIEC OPS Booklet (2004) Appendix A: Objective 5 p. A4-A5	The examiner should verify the organization has extended their segregation of duties processes to include their managing and operations AWS services. Additionally, the examiner should review and cross reference organizations data classification and access management policies, procedures and implementation for all systems to include AWS services. **Examiner should request and review** 1. The organizational data classification standards 2. Access Management policies and procedures 3. AWS Admin and User group configurations	Organizations should ensure adequate segregation of duties is defined and aligns with internal data classification standards and access management standards and configuration within both internal systems and AWS services.	AWS separates duties of individuals, as necessary, to prevent malevolent activity without collusion. Separation of duties is controlled through access controls, group permissions, logical access and change management processes. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-5 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 7
PE-3	Personnel Controls	Are there documented policies and procedures, which state dual administration control, segregation of duties, and employee background checks for employees with access to client information?	FFIEC OPS Booklet (2004) Appendix A: Objective 5 p. A4-A5	The examiner should verify the organization has included AWS services within their policies and procedures related to administrative configurations and dual control implementations. **Examiner should request and review** 1. Policies and procedures related to IT administration of internal systems and AWS services	Organizations should ensure policies and procedures are documented and in-place to support dual administrative control of internal systems and AWS services.	AWS separates duties of individuals, as necessary, to prevent malevolent activity without collusion. Separation of duties is controlled through access controls, group permissions, logical access and change management processes. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-5 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 7
PE-4	Personnel Controls	The organization should use employee-training programs to increase awareness of security issues and responsibilities.	FFIEC IS Booklet (2006) Appendix A: Objective 4.2	The examiner should check that the organization employee training programs and verify they define	Organization should ensure their internal security awareness program includes elements related to the use,	AWS has implemented a formal, documented awareness and training policy called “AWS Awareness and Training Policy,” that is reviewed and

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
			p. A5 FFIEC IS Booklet (2006) Appendix A: Tier II: F p. A16	security issues and responsibilities for internal systems and AWS services. **Examiner should request and review** 1. Employee security training policies and procedures	configuration and support of AWS services.	updated at least annually. The AWS Awareness and Training Policy is disseminated via the internal AWS Compliance web portal to all employees, vendors, and contractors. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AT-1 SOC 2 – Section III, Area B PCI DSS v3.0 Requirement 12
PE-5	Personnel Controls	Do all employees sign a statement of understanding acknowledging that they have read and understood company policies? Employees should be expected to understand and abide by rules concerning information confidentiality, nondisclosure, and the authorized use of information resources.	FFIEC IS Booklet (2006) Appendix A: Objective 4.2 p. A5 FFIEC IS Booklet (2006) Appendix A: Tier II: F p. A16	The examiner should check if all employees' sign a statement of understanding relate to information discloser, nondisclosure, and the authorized use of information resources, which include external services such as AWS. **Examiner should request and review** 1. Policies and Procedures related to information disclosure and authorized use of IT Services and AWS services	Organizations should ensure they have documented non-discloser agreements, which outline their responsibility within the use and administration internal systems and AWS services.	As part of the on-boarding process, all personnel supporting systems and devices within AWS sign a non-disclosure agreement prior to being granted access. Additionally, as part of orientation, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: PS-6 SOC 2 – Section III, Area B PCI DSS v3.0 Requirement 12
Change Management Controls						
CM-1	Change Management Controls	Has a proper change management process been deployed? It should include the following: - Change management processes, policies, procedures and forms - A change control oversight function to manage the overall change control process Additionally, management should formally define what constitutes a "change" and what	FFIEC OPS Booklet (2004) Appendix A: Objective 5 p. A4-A5 FFIEC D&A Booklet (2004) Appendix A: Objective 2, Objective 5, Objective 6, Objective 7 p. A2, A3-A6	The examiner should check that a change management process is in-place and changes related to AWS services are included, tracked and approved the same as internal change processes. **Examiner should request and review** 1. Policies and procedures related to change management 2. Sample change requests related to changes for AWS services	Organization should ensure change management process and practices for all AWS service components have been integrated into your existing policies, change management approval processes and management has visibility in the changes within the use of AWS services.	AWS has implemented a formal, documented configuration management policy, which is applicable to AWS, titled "AWS Configuration Management Policy". The AWS Configuration Management Policy is disseminated via the internal AWS Compliance web portal to all employees, vendors, and contractors. The AWS Compliance team reviews this policy annually, with approval by the AWS Chief Information Security Officer.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		standards should be observed to govern the change process.				**Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
CM-2	Change Management Controls	Does the change management procedure take into consideration: - Change request approval - Testing - Back out procedures - Change log - User training	FFIEC D&A Booklet (2004) Appendix A: Objective 10 p. A7-A8	The examiner should check that a change management process includes management of AWS service and changes to AWS services to include testing, back out procedures, training and logs related to changes. **Examiner should request and review** 1. Documented process elements related to testing, back out process and training related to AWS service changes	Ensure your use of AWS services follows the same change control processes as your internal series. For more information see: AWS Documentation	AWS service owners test, validate and document changes to systems and devices within AWS prior to implementing changes to the system and devices. Per the AWS Configuration Management Plan, service owners document the all aspects of changes in the CM tool, which include both the test / validation procedures related to each change. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
CM-3	Change Management Controls	Has a patch management process been deployed to approve and record changes due to patch updates? Do all patch deployments follow established change control procedures? All patch deployments should be documented. Management should stay abreast of all patches developed for systems under their responsibility. Patches should be installed and tested in segregated environments and installed when appropriate.	FFIEC OPS Booklet (2004) Appendix A: Objective 5 p. A4-A5 FFIEC D&A Booklet (2004) Appendix A: Objective 11 p. A8	The examiner should validate AWS services are included within the organizations internal patch management process. **Examiner should request and review** 1. Documented process for configuration and patching of AWS EC2 instances: • Amazon Machine Images (AMIs) • Operating systems • Applications	Organization should ensure AWS services in use are patch and configured based on established internal standards and procedures. Example of AWS client serves to include in patch deployment process: • Amazon Machine Images (AMIs) • Operating systems • Applications	Deploying patches provided by Amazon Stewards for the appropriate security fixes controls network and service flaw remediation maintenance. Amazon Stewards are responsible for reviewing the applicability, validity, and severity of security fixes before release for Service Groups to deploy. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: MA-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
CM-4	Change Management Controls	Patch management strategies should include establishing version control of all operating system and application software. All software and OS versions should be recorded and compared against the latest releases.	FFIEC OPS Booklet (2004) Appendix A: Objective 5 p. A4-A5 FFIEC OPS Booklet (2004) Appendix A: Tier II: A p. A11-A12	The examiner should check that patch management strategies include establishing version control of all operating systems, Amazon Machine Images and application software used within the AWS service environment. **Examiner should request and review** 1. Documented configuration standards (Gold images) of AWS EC2 instances: • Amazon Machine Images (AMIs) • Operating systems • Applications	Organization should develop approved configurations or baselines for AWS systems and services such as Amazon Machine Images, Operating systems and applications running on AWS. For more information on creating a customized Amazon Machine Image see: AWS AMI User Guides	All AWS systems maintain baseline configurations to devices in order to maintain configuration homogeneity throughout the fleet of network devices. In order to make changes to production devices or environments or deploy additional devices, a CM must be entered and approved in the CM tool. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
CM-5	Change Management Controls	Develop and document policies and procedures to ensure that modifications to client information systems are consistent with the service provider's Information Security Program.	FFIEC OT Booklet (2004) Appendix A: Tier II: D p. A10-A11	The examiner should check that policies and procedures related to client information within AWS is secured in accordance the organizations IT Security Policies **Examiner should request and review** 1. Information & Data protection policies and procedures for data hosted within AWS	Organizations should ensure their existing procedures for handling client information hosted in AWS services is consistently followed and aligned with existing IT security policies.	AWS employees are required to review and sign-off on an employment contract, which acknowledges their responsibilities to overall Company standards and information security, which includes processes for discloser of client information. Confidentiality agreements, which include information protection requirements, are reviewed and signed-off by all Amazon employees. **Reference**: ISO/IEC 27001:2005 Control: A.6.1.5 & A.7.1.3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
Systems Development Lifecycle						
SD-1	Systems Development Lifecycle	Are there well documented policies and procedures for systems acquisition, configuration and maintenance such as: - Risk assessment	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5	The examiner should verify that AWS services are integrated within the organizational SDLC process. **Examiner should request and review**	Ensure the use of AWS development tools (e.g. EC2Config, API tools & Command line tools) are documented and follow the same internal SDLC process as internally developed systems.	AWS Information Security team has responsibility for the information security of AWS and is the owner of the Secure Software Development Process.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		- Feasibility analysis - Testing - System development - System acquisition process (software and hardware) - Change management overview - Information system maintenance practices	FFIEC OPS Booklet (2004) Appendix A: Objective 5 p. A4-A5 FFIEC D&A Booklet (2004) Appendix A: Objective 5, Objective 6, Objective 7 p. A3-A6	1. The organizations use of AWS development tools to determine if they have been included into the SDLC policy and procedures		Development team roles and responsibilities for Security review are spelled out in the InfoSec Security Reviews policy and include registering the application, initiating the application risk classification, initiating the security review, participating in the architecture review and threat modeling and performing the code review. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SA-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
SD-2	Systems Development Lifecycle	Are there well-defined procedures and criteria for evaluating security requirements prior to development or acquisition of a system? Systems security requirements should be aligned to industry best practices and standards.	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: B, C, D, H p. A12-A16, A17-A19	The examiner should check that there are well-defined procedures and criteria for evaluating security requirements prior to development systems to be hosted within AWS. **Examiner should request and review** 1. The organizations SDLC policy and procedures 2. Procedures associated with the evaluation of AWS services and alignment with: AWS documentation	Organization should ensure they define procedures and documentation standards for the use and configuration of AWS services based on leading practices and recommendation within: AWS documentation	AWS Information Security team has responsibility for the information security of AWS and is the owner of the Secure Software Development Process. Development team roles and responsibilities for Security review are spelled out in the InfoSec Security Reviews policy and include registering the application, initiating the application risk classification, initiating the security review, participating in the architecture review and threat modeling and performing the code review. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SA-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
SD-3	Systems Development Lifecycle	Is there a formal configuration management program in place? Are all systems sufficiently hardened prior to release into production environments?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5	The examiner should check that there is a formal configuration management program in place and all systems are sufficiently hardened prior to release into production environments.	Organizations should develop defined Amazon Machine Images (AMI) for the services used within AWS	AWS has implemented a formal, documented configuration management policy, which is applicable to AWS, titled “AWS Configuration Management Policy”.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
				Examiner should request and review 1. Configuration examples of Amazon Machine Images (AMI) in use within the organization 2. Configuration of any AWS services according AWS security guidance, including logging, monitoring, permissions, and encryption key management	For more information on creating a customized Amazon Machine Image see: AWS AMI User Guides	**Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
Service Provider Oversight						
SPO-1	Service Provider Oversight	Are reasonable steps taken to select and retain service providers that are capable of maintaining appropriate safeguards for client information?	FFIEC IS Booklet (2006) Appendix A: Tier II: J p. A20 FFIEC OT Booklet (2004) Appendix A: Objective 3 p. A3-A7 FFIEC OT Booklet (2004) Appendix A: Tier II: B, D p. A8-A9, A10-A11	The examiner should check that reasonable steps are taken to select and retain service providers and the service provider is capable of maintaining appropriate safeguards for client information. **Examiner should request and review** 1. Organization vendor management and procurement processes to validate there are sufficient security reviews in place 2. IT risk management policies and procedures addressing external service providers 3. Evaluation documentation used to on-board AWS services	Organization should ensure they document and follow a defined process to evaluate, on-board and maintain security safeguards within their use of external service providers such as AWS.	AWS has implemented a formal, documented system acquisition planning policy called "AWS System and Services Acquisition Policy," that is updated and reviewed annually. The AWS System and Services Acquisition Policy is disseminated via the internal AWS Compliance web portal to all employees, vendors, and contractors. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SA-1 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12
SPO-2	Service Provider Oversight	Are there well-documented policies and procedures for vendor/service provider management?	FFIEC IS Booklet (2006) Appendix A: Objective 4, Objective 5 p. A4-A6 FFIEC OT Booklet (2004) Appendix A: Tier II: D p. A10-A11	The examiner should verify AWS service use is documented within policies and procedures for vendor/service provider management. **Examiner should request and review** 1. Organization vendor management policies and procedures for managing vendors and service providers	Organization should implement and documented policies and procedures for managing external service providers such as AWS. Procedures should outline on-boarding, shared security responsibility and communication processes between organization and service provider. (e.g. Incident Response, Disaster Recovery, Security notification, etc.)	Acquisitions for AWS are for hardware components and Commercial Off the Shelf (COTS) software. For purchases of COTS products and/or services, vendor claims of compliance to security requirements are required to be documented for consideration and practical testing during the technology evaluation phase. Once selected, AWS procurement requires that vendor contractual negotiations for technology/systems contain diagrams, drawings, and documentation as well as technical,

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
						security and business requirements specific to the procured technology. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SA-4 (1) SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12
SPO-3	Service Provider Oversight	If the service provider provides client information to any service providers or provides any service providers access to client information: a) Conduct appropriate due diligence in selecting service providers. b) Require all service providers to implement appropriate information security programs and measures. c) Regularly monitor service providers to confirm that they are maintaining appropriate security measures to safeguard client information.	FFIEC IS Booklet (2006) Appendix A: Objective 5 p. A5-A6 FFIEC IS Booklet (2006) Appendix A: Tier II: J, M p. A20, A22-A25	The examiner should check that there is a process to require service providers to adhere to appropriate due diligent standards, security program management and monitoring of service capability and reliability. **Examiner should request and review** 1. Organization vendor management policies and procedures 2. Service Level Agreements along with Key Performance Indicators (KPIs) defined for due diligence, security and monitoring	Organization should ensure their vendor management policies and procedures define appropriate due diligent, security and monitoring processes for external service providers such as AWS. Organization should define Service Level Agreements with Key Performance Indicators (KPIs) for service providers to follow and communicate their alignment with defined security and monitoring expectations.	AWS makes reasonable effort to select components validated to meet specific security and due care criteria and/or other requirements as appropriate to the proposed component being implemented. Proposed components or system enhancements are reviewed and coordinated amongst the Information Security Team, Development Team Manager, the appropriate Service Owner(s), and the Compliance Team for technical/business requirement satisfaction and security considerations, with the approval of the Information System Security Officer. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SA-4 (7) SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12
SPO-4	Service Provider Oversight	Does the entity maintain an inventory of current vendor/service providers and outsourcing relationships?	FFIEC IS Booklet (2006) Appendix A: Objective 1.3, Objective 2.1 p. A1-A2	The examiner should check that there is an inventory of current vendor/service providers and outsourcing relationships. **Examiner should request and review** 1. A listed of external service provider and service level agreements for current services	Organization should maintain an inventory of current vendor/service providers and outsourcing relationships. Specifically they should outline service interactions within AWS services along with communication channels.	AWS maintain a list of vendor and manufacturer documentation for external components, service provider and COTS software. AWS technical personnel supplement the vendor and manufacturer documentation with AWS specific documentation that describes the high-level design of the information system in terms of subsystems and

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
						implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SA-5 (3) SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12
SPO-5	Service Provider Oversight	Do you require your service providers by contract to implement and maintain privacy and security safeguards such as: a) Security responsibilities, controls, and reporting. b) Nondisclosure agreements with all service providers regarding impacted systems and data. c) Provisions for third-party reviews of the service provider's security through appropriate assessments and tests. d) Incident response procedures.	FFIEC IS Booklet (2006) Appendix A: Objective 5 p. A5-A6 FFIEC OT Booklet (2004) Appendix A: Objective 3 p. A3-A7	The examiner should check that service providers are required by contract to implement and maintain privacy and security safeguards such as: 1. Security responsibilities, controls, and reporting **Examiner should request and review** 1. A copy of the service providers SOC, ISO and other reports of compliance 2. Service Provider contracts with SLA, NDA and any disclosures related to data protection responsibilities	Organization should either establish and/or maintain a service provider oversight program which outlines shared responsibilities for security and data protections	AWS follows an established service provider program which follows several defined principals for agile acquisitions, small contracts, use of well recognized, established and diverse suppliers, multiple vendors, well-established suppliers, order direct from the manufacturer or through manufacturer certified and approved distribution partners. Additionally, AWS uses technologies, to the maximum extent possible as well as follows standard commercially available information system configurations. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SA-12 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12
Business Continuity Planning						
BCP-1	Business Continuity Planning	Is there a documented Business Continuity Plan (BCP) clearly stating objective and responsibilities? The BCP should be done on an enterprise-wide basis. The BCP should be about maintaining, resuming and recovering the business and not just recovery of the technology.	FFIEC BCP Booklet (2008) Appendix A: Objective 4.6, Objective 5 p. A6-A7 FFIEC OPS Booklet (2004) Appendix A: Objective 3	The examiner should check and review that AWS services are included into the organization BCP. The BCP should address the following areas relative to AWS services: 1. Use of AWS services for off-site backup 2. Use of AWS for interim operations	Organizations should ensure they have an established documented Business Continuity Plan, which includes AWS services in use across the organization. At a minimum the BCP should address the following areas relative to AWS services: 1. Use of AWS services for off-site backup.	AWS has implemented a formal, documented contingency planning policy, which is applicable to AWS, titled "AWS Contingency Planning Policy". The AWS Contingency Planning Policy is disseminated via the internal AWS Compliance web portal to all employees, vendors, and contractors. The AWS Compliance team reviews this policy annually, with approval by the AWS Chief Information Security Officer.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		Is a copy of the BCP distributed to the proper personnel and the recovery locations?	p. A3	3. Use of AWS BCP process support (BCP document storage, communications, etc.) 4. Use of AWS availability zones as interim operations for AWS services 5. Impact and strategy for AWS outages **Examiner should request and review:** 1. Copies of the organizations BC plan. 2. Verify AWS services in use have been properly identified and included 3. BCP distributed to the proper personnel and the recovery locations	2. Use of AWS for interim operations. 3. Use of AWS BCP process support (BCP document storage, communications, etc.). 4. Use of AWS availability zones as interim operations for AWS services. 5. Impact and strategy for AWS outages. Reference: Using Amazon Web Services for Disaster Recovery	**Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-1 SOC 2 – Section V
BCP-2	Business Continuity Planning	Has a Business Impact Analysis (BIA) and risk assessment been done to justify contingency plans?	FFIEC BCP Booklet (2008) Appendix A: Objective 3 p. A3-A4	The examiner should check that a Business Impact Analysis (BIA) and risk assessment have been done as well review if AWS services were included within the BIA. **Examiner should request and review:** 1. The BIA and/or risk assessment process and documentation 2. Risk Treatment plans as a result of the BIA 3. Project plans resulting from the BIA related to AWS services	Organizations should complete a Business Impact Assessment (BIA) or risk assessment at least every 12-18 months. The BIA should include any use of AWS services. Additionally, a risk treatment plan should be established and maintained with defined timeline, milestones and resources needed to remediate the risks identified.	The Amazon Web Services Contingency Plan (CP) lays out the processes and procedures used to respond to a serious outage or degradation of services at AWS. The AWS CP is applicable to AWS, as AWS is implemented as a specialized Region of AWS. Additionally, AWS conducts impact assessments during the weekly Capacity Management meetings at AWS. These meetings are attended by representatives of the IT Service Teams and are used to ensure that resources are acquired and allocated to meet system needs including ongoing operations and maintenance activities. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-2 (2) SOC 2 – Section V

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
BCP-3	Business Continuity Planning	Does the BCP take into account the following elements: - Personnel - Facilities - Technology (hardware, software, operational equipment) - Telecommunications/ networks - Vendors & service providers - Utilities - Data and records - Law enforcement - Media and Shareholders - Role of security within its BCP i.e. physical and logical access to the recovery site and computer systems	FFIEC BCP Booklet (2008) Appendix A: Objective 5 p. A6-A7	The examiner should check that the BCP includes AWS services, personnel and technologies used in support of the organizations operations and BC capabilities. **Examiner should request and review:** 1. BCP to ensure AWS services, technologies and shared responsibilities roles are documented	Organizations should ensure their BCP includes AWS services, technologies and region being used Additionally, organization should document the shared responsibilities between AWS and the organizational roles as they related to BCP.	The Amazon Web Services Contingency Plan (CP) lays out the processes and procedures used to respond to a serious outage or degradation of services at AWS Since new resources are continually being brought online to satisfy the demands of a rapidly growing client base. AWS employs an N+1 redundancy model. N+1 redundancy is a form of resilience that facilitates system availability in the event of component failure. Components (N) have at least one independent backup component (+1). AWS employs N+1 redundancy with active-active components, so the backup component is active in the operation even when all other components are fully functional. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-2 (2) SOC 2 – Section V
BCP-4	Business Continuity Planning	Does the BCP include the following emergency preparedness and crisis management aspects such as: - An employee/manager contact tree - Explains actions to be taken in specific emergency situations - Defines the conditions under which the back-up site would be used & has procedures in place for notifying the back-up site - Identifies sources of needed office space and equipment and list of key vendors (hardware/software/communications, etc.	FFIEC BCP Booklet (2008) Appendix A: Objective 5 p. A6-A7	The examiner should check that the BCP includes emergency preparedness and crisis management elements as outlined within the control and that these elements extend and/or include AWS services in use. **Examiner should request and review:** 1. The emergency and crisis management plan 2. Emergency communication plan to include initiate external services (i.e. AWS)	Organization should ensure they document and employ emergency and crisis action plans to respond to incidents and/or outages. Plan should include AWS services in-use day to day as well as AWS service, which may be used as part of a back-up recovery process.	The Amazon Web Services Contingency Plan (CP) lays out the processes and procedures used to respond to a serious outage or degradation of services at AWS. If the outage meets the criteria, the TOS engineer will start an engagement, which activates the ISCP. The TOS engineer will employ the Event Management Tool (EMT) system to start the Engagement and page problem resolvers. The TOS Engineer will initiate a conference call that all resolvers will join. The TOS engineer will initially assume the role of Call Leader.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		- Designates a public relations spokesperson				**Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-2 (2) SOC 2 – Section V
BCP-5	Business Continuity Planning	Are there adequate procedures in place to ensure that the BCP is maintained in a current fashion and updated regularly? Has a senior manager been assigned responsibility to oversee the development, implementation, testing, and maintenance of the BCP?	FFIEC BCP Booklet (2008) Appendix A: Objective 2 p. A3 FFIEC OPS Booklet (2004) Appendix A: Objective 3 p. A3	The examiner should check that there are procedures in place to ensure that the BCP is maintained and a senior manager has been assigned oversight responsibility. **Examiner should request and review:** 1. BC plan and verify it has been updated and a senior manager appointed oversight 2. Verify the BC plan has been updated for the use of AWS services	Organization should ensure their BC plan is current, includes AWS services and updated regularly. Additionally, a senior manager should be assigned oversight responsibility.	AWS has implemented a formal, documented contingency planning policy, which is applicable to AWS, titled "AWS Contingency Planning Policy". The AWS Contingency Planning Policy is disseminated via the internal AWS Compliance web portal to all employees, vendors, and contractors. The AWS Compliance team reviews this policy annually, with approval by the AWS Chief Information Security Officer. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-1 SOC 2 – Section V
BCP-6	Business Continuity Planning	Has the selection of recovery site and offsite storage taken into consideration geographic diversity?	FFIEC BCP Booklet (2008) Appendix A: Objective 4 p. A4-A6	The examiner should check if an offsite recovery and storage capability has been identified. For AWS services, they examiner should review the use of AWS availability zones and ensure organization understand their recovery responsibilities. Note: An AZ is a distinct location that is designed to be insulated from failures in other AZ's. **Examiner should request and review:** 1. Organization AWS architecture documentation and DR plans	Organization Identify the current AWS Regions and corresponding Availability Zones (AZs). Determine if a multi-AZ strategy deployment strategy was utilized for your organization's assets. AWS recommends that clients launch instances in more than one AZ to prevent loss of service in the event of a failure that affects an entire AZ. Additionally, review your organization's AWS architecture documentation, DR plans, and discussions with key DR personnel, identify the proposed DR approach at time of disaster.	AWS does not fit in the traditional model of backup tapes, offsite data storage and alternate processing sites. AWS has been built from the ground up to provide highly available computing and data storage combined with a redundant architecture to reduce the impact of outages. AWS services are designed to make use of the available storage and compute capacity. AWS does not employ an alternate storage site in a classic sense in its recovery model. Data within AWS is stored in multiple locations automatically by the EBS and S3 services. The offsite data storage is therefore implemented as online storage and the offsite location is simply another active AWS Data Center.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
						Reference: NIST SP 800-53 rev.3 FedRAMP Control: CP-6 SOC 2 – Section V
BCP-7	Business Continuity Planning	Does the BCP testing plan verify that all critical business units/departments/functions are included during the annual testing? Determine if the level of testing is adequate for the size and complexity of the organization.	FFIEC BCP Booklet (2008) Appendix A: Objective 10 p. A11-A15	The examiner should check that the BCP testing plan is inclusive of all services to include AWS services within use in the organization. **Examiner should request and review:** 1. The BCP testing plan 2. Test results reports 3. Verify AWS services are included within the plans and testing reports	Organization should ensure they have BCP test plans and AWS services are included in the testing processes. Additionally, organizations should determine if they should consider the single or multi-AZ deployment approach for your organization.	AWS BCP Testing consists of two types of exercises: Engagement Drills and Game Day Exercises. Engagement drills test the BCP procedures by selecting a simulated severity one or two event and activate the BCP by starting an engagement. Game Day exercises are full-scale functional BCP tests conducted annually. The difference between an Engagement Drill and a Game Day exercise is that the later includes inducing an actual failure to occur and cause production load shifts. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-4 SOC 2 – Section V
BCP-8	Business Continuity Planning	Determine if the DRP/BCP is tested annually.	FFIEC BCP Booklet (2008) Appendix A: Objective 10 p. A11-A15	The examiner should check that the BCP is tested at least annually and includes the use of AWS services. **Examiner should request and review:** 1. The BCP testing plan 2. Test results reports	Organization should ensure they have BCP test plans and AWS services are included in the testing processes. Testing should be conducted at least annually and documented.	AWS BCP Testing consists of two types of exercises: Engagement Drills and Game Day Exercises. Engagement drills test the BCP procedures by selecting a simulated severity one or two event and activate the BCP by starting an engagement. Game Day exercises are full-scale functional BCP tests conducted annually. The difference between an Engagement Drill and a Game Day exercise is that the later includes inducing an actual failure to occur and cause production load shifts. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-4 SOC 2 – Section V

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
Access Management, Authentication, and Authorization						
AAA-1	Access Management, Authentication, and Authorization	Is there a formal process for managing access to operating systems, network devices and applications, which should include procedures for: a) Creating new users b) Granting and revoking access rights c) Monitor access rights granted to each user d) Performing updates to access rights on each system or personnel change	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: A p. A8-A12	The examiner should review internal policies and procedures for managing access to AWS services and Amazon EC2 instances. **Examiner should request and review** processes for AWS managing access 1. Native AWS authentication methods 2. Federated authentication and connecting to a corporate Active Directory or; 3. LDAP implementation 4. IAM configuration – Export IAM Settings	The organization should document their use and configuration of AWS access controls examples and options outlined below: 1. Description of how Amazon IAM is used for access management. 2. List of controls that Amazon IAM is used to manage – Resource management, Security Groups, VPN, object permissions, etc. 3. Use of native AWS access controls or if access is managed through federated authentication using the organization's LDAP integration. 4. List of AWS accounts and Roles. 5. Provide a description of Amazon IAM accounts and roles, are monitoring methods. 6. Provide description and configuration of systems within EC2. Please refer to Amazon IAM documentation for implementation and best practices.	AWS has implemented a formal, documented access control policy called "AWS Access Control Policy," that is updated and reviewed on an annual basis (or when any major change to the system occurs that impacts the policy). The AWS Access Control Policy is disseminated via the internal AWS Compliance web portal to all employees, vendors, and contractors. The AWS Compliance team reviews this policy annually, with approval by the AWS Chief Information Security Officer. This policy addresses purpose, scope, roles, responsibilities, and management commitment. For additional resources and reports related to AWS access management See link: AWS Compliance Requests **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7
AAA-2	Access Management, Authentication, and Authorization	Users and system resources are assigned rights on the principles of Least privilege and 'need-to-know' that aligns with their required job functions.	FFIEC IS Booklet (2006) Appendix A: Tier II: A p. A8-A12	The examiner should review the type of access control in use within the organization as it relates to AWS services: **Federated Access Controls:** If federation authentication is used, the examiner should ensure that the mechanisms properly apply internal role assignments to AWS permissions	Organization should document the types access management, role and groups being used: 3. List of controls that Amazon IAM is used to manage – Resource management, 4. List of AWS accounts and roles.	AWS has implemented a formal, documented access control policy called "AWS Access Control Policy," that is updated and reviewed on an annual basis (or when any major change to the system occurs that impacts the policy).

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
				and understand the processes and methods to authorize access levels to ensure a least privilege model has been implemented. **Native AWS Access Controls:** The examiner should compare Amazon IAM roles and user assignment to functional roles and responsibilities. Temporary credentials should also be considered to ensure that these credentials are only assigned limited privileges. **Instance Access Controls:** For Amazon EC2 instances, the examiner should review implemented roles and assignments based on the local operating systems access controls mechanisms and/or any federation that the organization has established for managing access to the EC2 virtual machines. **Examiner should request and review** 1. Amazon IAM account plans 2. Amazon IAM settings	5. Provide processes to establishing and maintaining least privilege. 6. Provide information from EC2 environment application controls. Amazon IAM accounts, directly or via federation, should integrate with privilege management processes. Please refer to Amazon IAM documentation	All AWS system account is provisioned with minimal access in accordance with the principle of least privilege. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7
AAA-3	Access Management, Authentication, and Authorization	Are the records of access granted maintained in a central location?	FFIEC IS Booklet (2006) Appendix A: Tier II: M p. A22-A25	The examiner should review records for granting access to AWS services and Amazon EC2 instances. **Examiner should request and review** 1. Access requests related to AWS service provisioning 2. Requests should match to logged AWS API events – AWS CloudTrail	Amazon IAM accounts, directly or via federation, and EC2-resident control should integrate with privilege management processes. The organization should develop or extend processes to ensure that all access that is granted to users is properly documented and retained.	User accounts are established as part of the onboarding workflow process in Amazon's Human Resource Management System (HRMS). All employees, vendors, and contractors who require a user account must be on-boarded through Amazon's HRMS. As part of the onboarding workflow, the direct manager of the employee, vendor, or contractor requests the establishment of a user account. The approved request serves as the approval to establish a user account. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-6 SOC 2 – Section III, Area C

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
						PCI DSS v3.0 Requirement 7 & 10
AAA-4	Access Management, Authentication, and Authorization	Is there an adequate authentication process, such as user names and passwords that restricts access to the network, operating systems, network devices and applications?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: A p. A8-A12 FFIEC AUD Booklet (2012) Appendix A: Tier	The examiner should review the type of access control in use within the organization as it relates to AWS services. Additionally, review the user account policy and password complexities and validate that they extend to AWS services. **Examiner should request and review** 1. Access management policy and procedures 2. Amazon IAM settings	Organization should implement and maintain access control for EC2 instances and services within the EC2 environment, such as RDS. Just as stand-alone systems, you must implement and maintain access controls for these virtual systems either with local accounts or by connecting them to directory service for access control management.	AWS has implemented a formal, documented access control policy called "AWS Access Control Policy," System accounts are established by submitting a request using Amazon's self-service system account creation tool. Using this tool, mandatory fields, including unique account name, an account description, account owner, and a justification for the account creation. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-6 PCI DSS v3.0 Requirement 8
AAA-5	Access Management, Authentication, and Authorization	Has the organization implemented multi-factor authentication on all critical systems, services, and applications where risk demonstrates need such as remote access, non-console access, administrator access on core systems etc.?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5	The examiner should review the type of access control in use within the organization as it relates to AWS services. **Note: Native AWS Access Controls:** If the financial institution uses the AWS native security features, the examiner should perform the following steps. Identify documentation related to the process for granting access to new users and management approval. 1. Select a sample of AWS Management or Command Line access users 2. Review evidence of formal management approval for the assigned access **Examiner should request and review** 1. A sample of users that Multi-Factor identification is enabled by oobserving a user accessing the Management Console and determines if a token	A formal process should be developed for assigning new users with access to manage AWS services. This should include evidence of request, management approval and access granted to align with management's agreed upon access. Clients will need to assign each user a unique password and enable a Multi-Factor Authentication Device. This can be done by leveraging the IAM service with the following steps: 1. Open IAM service. 2. For each user, select the user account and select "Security Credentials". 1. Ensure that a password and multi-factor authentication devices is enabled for each user. For command line and API access, AWS requires that an Active Access Key and Signing Certificate be enabled. AWS Management Console, API and Command Line tools require encrypted	AWS administrators authenticate their SSH connection to the network bastion hosts using an RSA private key and passphrase, then log on to the network device which uses TACACS to authenticate the user with their LDAP user ID and password. For privileged (root) commands, users must escalate privileges using an authenticated password. All escalations of privilege commands are audited. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IA-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 8

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
				(virtual or physical) is requested 2. For Amazon EC2 instances, the examiner should review multi-factor authentication mechanisms in a similar manner as with physical systems	connections to perform the actions and cannot be changed. For more information on MFA see: Multi-Factor Authentication	
AAA-6	Access Management, Authentication, and Authorization	Does the organization enforce unique user ids for access to shared IT resources?	FFIEC IS Booklet (2006) Appendix A: Tier II: A p. A8-A12	The examiner should review a list of accounts within IAM and ensure that all users are required to use a unique user account and that no shared accounts exist to access the AWS environment. **Examiner should request and review** 1. List of configured user IDs and access configurations	Unique user accounts should be used for access AWS management console functions, AWS services, as well as instances and data stored within EC2, RDS, S3 or other services. In a federated environment, this can be accomplished by assigning unique accounts in the organization's LDAP implementation and only assigning AWS rights to accounts that are individually assigned. Within IAM, organizations can create unique user accounts for each individual that will require access and assign appropriate authorization to each account.	AWS has implemented a formal, documented access control policy called "AWS Access Control Policy," System accounts are established by submitting a request using Amazon's self-service system account creation tool. Using this tool, mandatory fields, including unique account name, an account description, account owner, and a justification for the account creation. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-6 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7
AAA-7	Access Management, Authentication, and Authorization	Does the organization enforce strong password requirements such as a minimum of 8 characters, password complexity, rotation every 42 days etc.?	FFIEC IS Booklet (2006) Appendix A: Tier II: A p. A8-A12 FFIEC EB Booklet (2003) Appendix A: Objective 4.5 p. A11-A12	The examiner should review internal policies and procedures for enforcing strong passwords to AWS services and Amazon EC2 instances **Examiner should request and review**: 1. The process for enforcing password policies includes access to AWS management capabilities and Amazon EC2 instances	Organization should define strong password requirements and ensure they extend to AWS service If Amazon IAM is not able to enforce password requirements for complexity, rotation, or expiration, then the client must implement additional controls, Amazon IAM Multi-Factor Authentication should be enabled for these accounts. Implement and maintain access control for EC2 instances and services within the EC2 environment, such as RDS. Just as stand-alone systems, you must implement and maintain access	AWS enforces password complexity in the AWS LDAP with the AWS Password tool, which is employed by users to change passwords. This mandates that passwords: 1. Are case sensitive 2. Must be 8 to 30 characters long and contain at least one uppercase letter, one lowercase letter and one non-alphabetic character that is not the first or last character 3. Cannot be a password that the user has previously used

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
					controls for these virtual systems that enforce password controls.	**Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IA-5 SOC 2 – 'Security Procedures' Criteria 3.2 PCI DSS v3.0 Requirement 8
Network Controls						
NW-1	Network Controls	Is the telecommunications infrastructure designed with redundancy in mind? Single points of failure should be carefully scrutinized and eliminated.	FFIEC OPS Booklet (2004) Appendix A: Objective 8 p. A6-A7	The examiner should review overall infrastructure, including the connection to and use of AWS services. AWS provides redundancy features, such as Availability Zones and redundant Direct Connect or Amazon EC2 VPN. The examiner should review the implementation of these features to eliminate single points of failure. **Examiner should request and review**: 1. The configuration of Amazon EC2 instances and services within ECS, such as Amazon RDS for redundancy	Organization should review their infrastructure redundancy requirements and ensure they review their use of AWS services to ensure there is no single point of failure. Most AWS services have availability options using Availability zones. Each service must be considered to provide a comprehensive redundancy design. AWS services may also provide redundancy for other infrastructure that is currently used as primary sites for systems.	AWS employs an n+1 redundancy model. N+1 redundancy is a form of resilience that ensures system availability in the event of component failure. Components (N) have at least one independent backup component (+1). AWS employs N+1 redundancy with active-active components, so the backup component is active in the operation even if all other components are fully functional. This is applied throughout AWS including network and data center implementation. Data center network ingress/egress is architected with diverse paths using alternate service providers. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-2 SOC 2 – Section III, Area C
NW-2	Network Controls	Are logical domains and network segmentation used to group users, network servers, applications, and data into separate security domains?	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14 FFIEC AUD Booklet (2012) Appendix A: Tier II: D A13-A14	The examiner should review AWS Security Group implementation, AWS Direct Connect, and Amazon VPN configuration. AWS provides native and inherent controls for instance isolation and these controls are maintained through the use of the AWS Security Groups. **Examiner should request and review**: 1. Segmentation controls for physical devices and systems connecting to	AWS provides client configurable Security Groups to describe and implement network segmentation. Additional options, such as VPC may be used to further define system boundaries and provide a virtual private cloud environment to manage any sensitive client information.	The AWS Access Control Policy mandates that access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by AWS to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. **Reference**:

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
				Amazon EC2 and other AWS services		NIST SP 800-53 rev.3 FedRAMP Control: CP-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
NW-3	Network Controls	Are access controls such as ACL's and firewalls deployed to restrict actions within and between each security domain?	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should review AWS Security Group rules, AWS Direct Connect, and Amazon VPN configuration. **Examiner should request and review**: 1. ACL and firewall setting for AWS services	Organization should use AWS Security Groups to describe and implement network segmentation and ACLs. If AWS Direct Connect or VPC VPN is used, ensure that segmentation is properly configured for on-premises devices. Reference: AWS Security Groups	Systems and devices within the system boundary are segregated into separate rooms as deemed necessary. Servers and network devices are installed in server and networking rooms physically partitioned from rooms containing devices that provide power, HVAC and other environmental support to systems and devices within the system boundary. In addition, AWS has partitioned its internal network into two distinct network fabrics—PROD and EC2. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SC-32 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
NW-4	Network Controls	IT management should implement a layered approach to logical security controls that contain (at a minimum), preventative, detective, and corrective strategies. This would include access controls, logging and monitoring controls, and incident response controls.	FFIEC OPS Booklet (2004) Appendix A: Objective 5 A4-A5 FFIEC AUD Booklet (2012) Appendix A: Tier II: D A13-A14	The examiner should review AWS Direct Connect and Amazon VPN configuration. AWS also offers monitoring services, such as AWS CloudWatch and Describe API. If these are used, the examiner should review their use for logical security. **Examiner should request and review**: 1. Logging, monitoring, and alerting for physical devices hosted by the organization and systems connecting to Amazon EC2 and other AWS services 2. Logged AWS API events – AWS CloudTrail	The organization will need to establish appropriate logging and monitoring for EC2 instances to ensure that any possible security related events are identified. Although AWS manages a range of layered security controls for the AWS management environment, the organization will need to ensure that the configurations, assigned access, AWS Security Groups and EC2 instances have had proper controls implemented to ensure the layered approach has been properly implemented. Reference: • Service Access Logging • AWS CloudTrail • AWS Config	AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise occurs based upon threshold alarming mechanisms determined by AWS Service and Security teams. AWS monitoring includes devices such as firewalls, gateways, and routers. The monitoring tools all feature near real-time alerts. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SI-4 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1, 10, & 11

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
NW-5	Network Controls	Written procedures govern the daily activities of personnel responsible for maintaining the network and systems.	FFIEC AUD Booklet (2012) Appendix A: Tier II: D A13-A14	The examiner should verify that the procedures for governing the daily activities of personnel include AWS management capabilities and Amazon EC2 instances. **Examiner should request and review**: 1. Procedure for daily network and system activities to include the administration of the AWS services	Organizations should ensure that the procedures for governing the daily activities of personnel include AWS management capabilities and Amazon EC2 instances.	AWS has implemented a formal, documented system maintenance policy called "AWS Maintenance Policy," which is updated and reviewed annually. The AWS Maintenance Policy is disseminated via the internal AWS Compliance web portal to all employees, vendors, and contractors. This policy addresses purpose, scope, roles, responsibilities, and management commitment. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: MA-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
NW-6	Network Controls	Adequate approvals are required before deployment of remote, Internet, or VPN access to the network for employees, vendors, and others.	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14 FFIEC AUD Booklet (2012) Appendix A: Tier II: D A13-A14	The examiner should verify that the procedures are in place for deploying services within the organization **Examiner should request and review**: 1. Procedures for approval of remote access for employees, vendors, or other and ensure that they include access to AWS services and Amazon EC2 instances	Organizations should develop procedures for granting remote, Internet or VPN access to employees and should be extended to include AWS Console access and remote access to EC2 networks and systems.	Configuration-controlled to systems and devices within the system boundary require approval. For all changes deployed to systems and devices within the system boundary, at least two approvals are required. Inherent in these approvals are the explicit consideration for security impact analyses by the approvers. Approvers note their approvals within the CM ticket associated with the change. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1 & 6
Operating System Access						
OS-1	Operating System Access	Does the organization restrict access to all operating systems	FFIEC IS Booklet (2006)	The examiner should review internal policies and procedures for restricting	Organizations should consider AWS console and management access as	AWS implements least privilege throughout its infrastructure

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		utilities and configuration management to designated systems administrators?	Appendix A: Tier II: C p. A15-A16 FFIEC AUD Booklet (2012) Appendix A: Tier II: D A13-A14	access to AWS services and Amazon EC2 instances to designated administrators. **Examiner should request and review**: 1. That the process for restricting access to operating system utilities and configuration management includes access to AWS management capabilities and Amazon EC2 instances	administrative access and access to the various functions in the management console should be limited to designated system administrators. EC2 instances should be treated like any other operating system that is currently managed by the organization. The operation system should have similarly restricted access to systems utilities and configuration management of EC2 instances to administrators.	components. Network devices and servers are implemented with minimal functionality and service teams add only software packages and services needed for the device to perform its function. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7
OS-2	Operating System Access	Does the organization restrict and monitor all privileged or administrative access?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: A p. A8-A12 FFIEC AUD Booklet (2012) Appendix A: Tier II: D A13-A14	The examiner should review internal policies and procedures for restricting and monitoring privileged access to AWS services and Amazon EC2 instances to designated administrators. AWS also offers monitoring services, such as AWS CloudWatch and Describe API. If these are used, the examiner should review their use for logical security. **Examiner should request and review:** 1. Policies and procedures related to access management 2. Logging, monitoring, and alerting for Amazon EC2 instances	Organization should restrict privileged access to AWS service configuration using Amazon IAM. Although AWS logs and monitors access to the AWS console, they do not provide an interface for access the administrator logs to monitor administrator activities. A process must be established to periodically monitoring service configuration changes.	Access and Privileged Command Auditing Log (authpriv): The authpriv logs generated by AWS Linux systems record every automated and interactive login to the systems as well as every privileged command executed. At least weekly, the AWS Security team extracts all log messages related to these accesses, and provide reports to the AWS CISO, and VP, on a per-host class basis. Only employees with a business need to interact with production servers should be doing so, and only in the course of doing their jobs. In particular, the log analysis searches for events. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AU-6 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7, 10, & 11
OS-3	Operating System Access	The organization should ensure that access to all operating system parameters is restricted, i.e. normal users should not be granted local administrator rights unless justified by a business need.	FFIEC IS Booklet (2006) Appendix A: Tier II: A p. A8-A12	The examiner should review internal policies and procedures for restricting access to AWS services and Amazon EC2 instances to designated administrators. AWS Console and management API have equivalent function and sensitivity as physical	Organization should ensure all AWS console and management access is considered administrative access and access to the various functions in the management console should be limited to designated system administrators.	AWS implements least privilege throughout its infrastructure components. Network devices and servers are implemented with minimal functionality and service teams add only software packages and services

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
				systems, operating systems, and applications. Amazon EC2 instances should be regarded as equivalent to physical servers. **Examiner should request and review** 1. The process for restricting access to operating system parameters includes access to AWS management capabilities and Amazon EC2 instances		needed for the device to perform its function. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7
OS-4	Operating System Access	Are unauthorized attempts to gain access to the operating and application systems recorded, monitored, and responded to by independent parties?	FFIEC IS Booklet (2006) Appendix A: Tier II: A, B p. A8-A14 FFIEC OPS Booklet (2004) Appendix A: Tier II: F p. A14-A15	The examiner should review internal policies and procedures for monitoring access attempts AWS services. **Examiner should request and review:** 1. The EC2 instance configuration to validate that the system is configured to log and alert on unauthorized access attempts	Organization should restrict access to AWS service configuration using Amazon IAM. Although AWS logs and monitors access to the AWS console, they do not provide an interface to access the logs to monitor for unauthorized access attempts.	All access attempts to the bastion hosts by AWS administrators are logged, and the logs are reviewed by the Security team for unauthorized attempts or suspicious activity **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 10 & 11
OS-5	Operating System Access	Are assessment events enabled on all operating systems to log system activities?	FFIEC OPS Booklet (2004) Appendix A: Tier II: B, F p. A12, A14-A15 FFIEC AUD Booklet (2012) Appendix A: Tier II: D p. A13-A15	Examiner should review the Amazon EC2 instances in use within the organization. **Examiner should request and review:** 1. Logging of assessment events for all operating system parameters are implemented by reviewing the operating system configuration	Organization should restrict access to AWS service configuration using Amazon IAM. Although AWS logs and monitors access to the AWS console, they do not provide an interface to access the logs to monitor for unauthorized access attempts.	AWS implements least privilege throughout its infrastructure components. Network devices and servers are implemented with minimal functionality and service teams add only software packages and services needed for the device to perform its function. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 10
Application Access Controls						
AP-1	Application Access Controls	Authentication and authorization methods for applications should be sufficiently complex in	FFIEC OPS Booklet (2004) Appendix A: Tier II: G	The examiner should review authentication and authorization methods for applications implemented	The organization should determine which application or system processes access AWS services via APIs and AWS software development kits.	Application access controls are solely a client responsibility.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		accordance to the risk of the application.	p. A17	on Amazon EC2 instances in a similar manner as with physical systems. **Examiner should request and review:** 1. Access Management policies and procedure to include application level access within AWS services	If application or system processes require access to AWS resources, ensure access is provisioned securely and according to policy and document your understanding. The three types of access credentials are: 1. Signing symmetric encryption keys (for access via REST/Query APIs and third-party tools) 2. X.509 certificates and associated private keys (for access via SOAP APIs and command lines) 3. Multi-factor authentication (optional)	
AP-2	Application Access Controls	Are application access controls based on the principles of "least privilege" and "need-to-know"?	FFIEC IS Booklet (2006) Appendix A: Tier II: A p. A8-A12	The examiner should review application access controls implemented on Amazon EC2 instances in a similar manner as with physical systems. **Examiner should request and review:** 1. Access Management policies and procedure to include application level access within AWS services 2. Permission configuration for RDS databases	The organization should Implement and maintain access control for applications implemented on EC2 instances that are appropriate for the risk of the application and the needs of the organization users. Management of these controls should be integrated within the organizations existing access control processes.	Application access controls are solely a client responsibility.
AP-3	Application Access Controls	Are assessment events on applications enabled to log all access and security events?	FFIEC OPS Booklet (2004) Appendix A: Tier II: G p. A17 FFIEC OPS Booklet (2004) Appendix A: Tier II: B, F p. A12, A14-A15	The examiner should review assessment event logging for applications implemented on Amazon EC2 instances in a similar manner as with physical systems. **Examiner should request and review:** 1. Event logging policies and procedure to include application level access within AWS services	The organization should provide a description of application logging for applications implemented on EC2 instances.	Application access controls are solely a client responsibility.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
				2. Logging for RDS databases		
AP-4	Application Access Controls	Do business owners/unit managers assigned to each application possess ultimate discretion over users and data consumers given access to the application?	FFIEC IS Booklet (2006) Appendix A: Tier II: G p. A17	The examiner should verify internal policies and procedures for managing access to application include AWS services and Amazon EC2 instances. **Examiner should request and review:** 1. Policies and procedures for application access hosted within AWS and RDS databases	Organization should document application access and ownership for application hosted within AWS services.	Application access controls are solely a client responsibility.
AP-5	Application Access Controls	Do business owners regularly review access rights for all applications under their ownership?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5	The examiner should verify internal policies and procedures for managing access to application include AWS services and applications hosted within Amazon EC2 instances. **Examiner should request and review:** 1. Policies and procedures for application access hosted within AWS	Organization should ensure users and permissions for applications on EC2 instances and should be integrated with general access control processes.	Application access controls are solely a client responsibility.
Database Security Controls						
DC-1	Database Security Controls	Is database administrative access and data modification activities logged and closely monitored? These logs should not be subject to alteration by any member of the database administration group.	FFIEC OPS Booklet (2004) Appendix A: Objective 10 p. A8-A9 FFIEC OPS Booklet (2004) Appendix A: Tier II: F p. A14-A15	The examiner should review access and data modification activity for Amazon RDS or client databases is in a similar manner as with internal systems. **Examiner should request and review:** 1. Database administration policies & procedures to ensure they extend to AWS services use	Organization should Restrict access to AWS database configuration using Amazon IAM. Just as physical systems, you must implement and maintain controls for monitoring administrative access of databases within the AWS environment by configuring the system to log and alert on specified activities.	AWS administrators employ the Password Tool to associate an RSA public key with their system account. This public key is propagated to all hosts in the host classes that the user has permissions to manage. This allows the administrator to SSH to the hosts with their user id and the RSA private key, which the user maintains, protected by a passphrase. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-17 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 3

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
DC-2	Database Security Controls	When production data is utilized in test environments, security controls over access to the data should be as strong as the production environment. If not, management should implement controls that encrypt production data into test systems to protect data sensitivity.	FFIEC D&A Booklet (2004) Appendix A: Objective 9 p. A6-A7	The examiner should determine If production data is utilized in test environment using AWS database services, the examiner should review security controls for test databases. **Examiner should request and review:** 1. Security policies, procedures and controls for test databases in use within AWS services	If production data is used in test environments implemented by AWS, ensure that security policies, procedures and controls are configured to match production controls.	This control is solely a client responsibility.
Remote Access						
RA-1	Remote Access	Is remote access granted approval from management have a compelling business justification? Remote access, support, and administration should be carefully considered if not disallowed. At a minimum, administrators should require strong authentication and encrypted sessions?	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14 FFIEC AUD Booklet (2012) Appendix A: Tier II: D A13-A14	The examiner should review internal policies and procedures for managing access to AWS services and Amazon EC2 instances. If the organization is using Direct Connect to connect between their existing networks and AWS, the examiner should also review the remote access model used to access systems within the organization's network and if that remote access could be used for accessing systems within AWS. Note: All access to AWS and Amazon EC2 instances is "remote access" by definition unless Direct Connect has been configured. **Examiner should request and review:** 1. Policies and procedures for managing direct and remote access and validated AWS services align to them	Organization should implement and maintain remote access remote access for AWS services and instances. Assess Multi-Factor Authentication (MFA). Determine whether multi-factor authentication of AWS accounts is required by your policies. 1. If required, check the AWS Management Console to determine whether MFA is enforced on the AWS account and individual IAM user accounts. 2. Just as stand-alone systems, you must implement and maintain access controls for these virtual systems. This may include implementation of multi factor authentication. Reference: Multi-Factor Authentication	AWS remote administrative connections to the AWS system are performed using SSH. Remote connections are used to manage and operate the system. AWS administrators employ the Password Tool to associate an RSA public key with their system account. This public key is propagated to all hosts in the host classes that the user has permissions to manage. This allows the administrator to SSH to the hosts with their user id and the RSA private key, which the user maintains, protected by a passphrase. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-17 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 8
RA-2	Remote Access	All remote access should be logged and monitored.	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should review remote access logging for Amazon EC2 instances and IAM authentication configuration. Amazon IAM accounts for network access should be configured for multi-factor	Access to the AWS Management Console is logged and monitored by AWS. If direct access by allowing access to common management ports (i.e. 3389 for Windows or 22 for Linux) to EC2 instances is configured, logging	AWS employs automated mechanisms to facilitate the monitoring and control of remote access methods, through syslog running on the bastion hosts. Auditing occurs on the systems and devices within the sys.log or auth.log

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
			FFIEC AUD Booklet (2012) Appendix A: Tier II: D A13-A14	authentication. **Examiner should request and review:** 1. Access logging and IAM configurations	and monitoring should be configured in the systems to log all remote access in the operating system configuration.	files, which are then aggregated and stored for review and incident investigation. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-17 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 8
RA-3	Remote Access	All remote access communications should using strong authentication controls and encryption technologies.	FFIEC IS Booklet (2006) Appendix A: Tier II: B, K p. A12-A14, A20-A21	The examiner should review If Security Groups are configured to allow for direct access to common management ports (i.e. 3389 for Windows or 22 for Linux) for Amazon instances. Additionally, the examiner should review multi-factor authentication mechanisms and encryption configuration that may have been implemented on the system in a similar manner as with physical systems. **Examiner should request and review:** 1. AWS Security group configurations	All access to AWS Console and management uses HTTPS with strong encryption. If encryption of data in transit is required, identify whether connections to all applicable AWS services are via secure endpoints for HTTPS transmission. 1. Also determine the use of Windows X.509 certificates, SSH, SSL/TLS wrappers for native database protocols, and/or VPN solutions. 2. Understand and verify documentation around the protection of data in transit when managing AWS services	Remote access to hosts is via certificate-based SSH v2, which utilizes cryptographic hashes and ciphers to protect the confidentiality and integrity of remote access sessions **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-17 (2) SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 4
Personnel Control and Segregation of Duties						
PCS-1	Personnel Control and Segregation of Duties	Do system, network, and security administrators have minimum transactional abilities?	FFIEC IS Booklet (2006) Appendix A: Tier II: A p. A8-A12	The examiner should review the type of access control in use within the organization as it relates to AWS services: **Federated Access Controls:** If federation authentication is used, review internal role assignments to AWS permissions and understand the processes and methods to authorize.	Organization should document and list the control in place for managing: 3. Amazon IAM is used to manage – Resource management, Security Groups, VPN, object permissions, etc. 4. List of AWS accounts and roles. 5. If identity federation or temporary credentials are	All AWS personnel supporting systems and devices within the system boundary are classified as high-risk designations within AWS' parent organization, Amazon.com. These personnel are considered as having positions having access to sensitive AWS trade secrets, confidential or proprietary information or other valuable company assets.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
				Native AWS Access Controls: Amazon IAM roles and user assignment to functional roles and responsibilities. **Instance Access Controls:** For Amazon EC2 instances, review implemented roles and assignments based on the local operating systems access controls mechanisms and/or any federation that the organization has established for managing access to the EC2 virtual machines. **Examiner should request and review** 1. Amazon IAM account plans 2. Export Amazon IAM settings.	used, provide description of implementation. 6. Provide processes to establishing and maintaining least privilege. 7. Provide information from EC2 environment application controls. Implement and maintain access control for EC2 instances and services within the EC2 environment, such as RDS. Just as stand-alone systems, you must implement and maintain access controls for these virtual systems.	**Reference**: NIST SP 800-53 rev.3 FedRAMP Control: PS-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7
PCS-2	Personnel Control and Segregation of Duties	IT staff should be aware of the information security program and how it relates to their job functions. This includes security training programs and communicating security concerns and goals.	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC OPS Booklet (2004) Appendix A: Tier II: F p. A14-A15	The examiner should review information security awareness training records and verify that the training includes AWS security, such as Amazon IAM usage, EC2 Security Groups, and remote access to EC2 instances. **Examiner should request and review** 1. Security Awareness policies and procedures	The organization should ensure Information security awareness training include AWS security, such as Amazon IAM usage, EC2 Security Groups, and remote access to EC2 instances.	AWS has implemented a formal, documented awareness and training policy called "AWS Awareness and Training Policy," that is reviewed and updated at least annually. The AWS Awareness and Training Policy is disseminated via the internal AWS Compliance web portal to all employees, vendors, and contractors. The AWS Compliance team reviews this policy annually, with approval by the AWS Chief Information Security Officer. This policy addresses purpose, scope, roles, responsibilities, and management commitment. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AT-1 SOC 2 – 'Security Communications' Criteria 2.2 description PCI DSS v3.0 Requirement 12

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
PCS-3	Personnel Control and Segregation of Duties	IT security personnel that monitor the system and security administrator logs should function independently from IT operations, or implement appropriate compensating controls (i.e. outsourced security monitoring.)	FFIEC OPS Booklet (2004) Appendix A: Objective 5 p. A4-A5 FFIEC AUD Booklet (2012) Appendix A: Tier II: D A13-A14	The examiner should verify internal policies and procedures for managing access to AWS services and Amazon EC2 instances. Individuals monitoring security administrator logs should function independently from individuals responsible for operations administrators. **Examiner should request and review** 1. Access management policies and procedures 2. Logging and Monitoring policies and procedures	Organization should evaluate their use of direct or via federation access is implemented with the appropriate segregation of duties for administrator logs. Implement and maintain access control for EC2 instances. Log management configuration should enforce appropriate segregation of duties for security administration logs.	AWS segregation of duties is implemented and controlled via the management of information system accounts, group membership and group permissions. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-5 SOC 2 – 'Security Communications' Criteria 2.2 description PCI DSS v3.0 Requirement 12
Firewall Controls						
FC-1	Firewall Controls	Are all firewall rules approved by the ISO/steering committee or senior management? Is a record of all approval maintained?	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should verify internal policies and procedures for approving firewall rules include AWS Security Groups and VPN configuration. AWS Security Groups should be reviewed and validated against a sample of changes to ensure that appropriate approvals have been obtained. **Examiner should request and review** 1. Policies and procedures for firewall, security group and VPN configuration	Organization should define processes for firewall rules management with in AWS and should include Security Group configuration changes and management approval along with maintenance of documentation of the approval. If additional firewall technologies such as host-based or appliance-based firewalls are implemented in the EC2 environment, changes to these firewalls should also be approved and retained as well as the Security Groups documentation.	All compute instances have a host-based firewall in order to protect them from unintended or unauthorized connections and communications. AWS uses automated mechanisms to enforce both logical and physical access restrictions. These mechanisms support auditing of the enforcement actions. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SC-7 (12); CM-5 (1) SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
FC-2	Firewall Controls	Is the firewall configuration hardened to remove any unnecessary services and kept up-to-date with the latest security patches and firmware updates?	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should review the host-based or other firewall configuration to ensure it is properly hardened, and works with the organization to identify any vendor or industry documentation on hardening the firewall technology. **Examiner should request and review** 1. Policies and procedures for firewall, security group and VPN configuration	Organization should configure AWS Security Groups to align with their internal boundary protection policies. If other technologies such as host-based or other firewall technologies are implemented, the organization should ensure that the firewall configuration is hardened using vendor or industry standards such as NIST, CIS or SANS.	AWS implements least privilege throughout its infrastructure components. All network devices, firewalls and servers are implemented with minimal functionality and service teams add only software packages, patches and services needed for the device to perform its function. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
						SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1 & 2
FC-3	Firewall Controls	Are these firewall controls in place? a) Default, should restrict all traffic that is not specifically allowed b) Uses NAT to hide internal address c) Blocks malicious code d) Logging is enabled	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should verify If AWS Security Groups are the primary firewall solution. The AWS firewalls: a) Restrict all traffic by default b) Use NAT c) Implement stateful inspection d) Logs ACL and privilege use If other firewall technologies are used, the examiner should review the technology to ensure that it is properly configured to hide internal addresses, block malicious code and has logging enabled. **Examiner should request and review** 1. Policies and procedures for firewall, security group and VPN configuration	Organization should configure AWS Security Groups to align with their internal boundary protection policies. AWS ECS provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny mode and EC2 clients must explicitly open any ports to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or CIDR block). The firewall is controlled not by the host/instance itself, but requires the client's X.509 certificate and key to authorize changes, thus adding an extra layer of security. Within EC2, the client host administrator and client cloud administrator can be separate people, permitting two-man rule security policies to be enforced.	AWS Firewalls have a default deny all policy, so the instance owner must specifically define any access. AWS implements separate VLANs for each client in VPC, with the client controlling the VLAN configurations within their VPC. AWS NATs all traffic and prohibits all ports and protocols that do not have a specific business purpose. AWS provides audit record generation capability for auditable events for all security devices and hosts that offer auditing capability. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-5 & CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
FC-4	Firewall Controls	Is remote administration of the firewall performed only from secure devices, over trusted network paths, and with encrypted communications?	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should review AWS Security Group administration is performed from secure workstations and via HTTPS for either the AWS Console or command line API. Additionally, the examiner should review the multi-factor authentication is enabled for any user that is assigned general administrative rights or rights to manage security groups within the AWS Console or through command line APIs. **Examiner should request and review:** 1. Policies and procedures for managing remote access	Organization should implement HTTPS for AWS Management Console or command line API for managing the firewall. Additionally, organization should implement Multifactor authentication should be enabled for any user that is assigned general administrative rights or rights to manage security groups within the AWS Console or through command line APIs.	AWS remote administrative connections to the AWS system are performed using SSH v2. AWS administrators employ the Password Tool to associate an RSA public key with their system account. This public key is propagated to all hosts in the host classes that the user has permissions to manage. This allows the administrator to SSH to the hosts with their user id and the RSA private key, which the user maintains, protected by a passphrase. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AC-17 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
FC-5	Firewall Controls	Is administrative access to firewalls restricted to select IT staff?	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should verify internal policies and procedures for restricting AWS Security Group management to select IT staff. Ensure internal policies and procedures restrict AWS Security Group management to select IT staff. **Examiner should request and review** 1. Policies and procedures for firewall, security group and VPN configuration	If AWS services are used for client data, then AWS accounts that permit changes to Security Group configuration or VPN firewall rules of AWS permissions must be considered critical. Amazon IAM Multi-Factor Authentication should be enabled for these accounts. Additionally, consider using temporary security credentials (tokens) to avoid maintaining persistent privileged accounts.	AWS implements least privilege throughout its infrastructure components. All network devices, firewalls and servers are implemented with minimal functionality and service teams add only software packages, patches and services needed for the device to perform its function. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
FC-6	Firewall Controls	Firewall configuration changes should be conducted through a well-organized and documented change control procedure.	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should verify internal policies and procedures for firewall configuration changes include AWS Security Groups and VPN configuration. **Examiner should request and review** 1. Policies and procedures for firewall, security group and VPN configuration	Organizations should establish or extend from existing change processes to ensure that all firewall changes require appropriate change management processes and documentation.	The baseline configuration of network devices within the system boundary is maintained and updated by the Networking team. When updates are made to configurations, the Networking team employs the configuration management tools listed above to provide: 1. Version control - all updates are version controlled and previous version are available as needed 2. Access control - the user making the changes has permission to do so and changes are associated with a specific user 3. Documentation - the purpose of the change is captured The new baseline configurations are deployed to devices in order to maintain configuration homogeneity throughout the fleet of network devices. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1 & 2

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
FC-7	Firewall Controls	Does the organization document a firewall policy that describes the firewall's role in implementing the overall organizational security policy?	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should verify internal firewall policies include AWS Security Groups and VPN implementation and management. **Examiner should request and review** 1. Security policies to ensure firewall, security group and VPN management are defined	Organization should review and revise existing policies to include AWS Security Groups and VPC Firewalls management within their existing security policies.	AWS has implemented a formal, documented configuration management policy, which is applicable to AWS, titled "AWS Configuration Management Policy". The policy includes network and firewall roles and configurations. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CM-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
FC-8	Firewall Controls	Does the organization train their IT staff to ensure that the firewall policy is implemented properly, or ensure outsourced service delivery for firewall management complies with the organizational policy?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5	The examiner should review training records and verify that the training includes AWS security, such as Amazon IAM usage, EC2 Security Groups, and remote access to EC2 instances. **Examiner should request and review** 1. Security training program to ensure it includes AWS service support and security	Organization should review and revise existing procedural documentation and training materials to ensure that AWS firewalls are included in any awareness and training programs for IT Staff.	Role-based security training is required when significant changes have been made to system design/architecture, key system functionalities, and significant organizational changes. Additionally, role-based training is provided on an ongoing basis via day-to-day interaction and reviewing the team wiki. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AT-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
Logging, Assessment Trails, and Monitoring						
LAM-1	Logging, Assessment Trails, and Monitoring	Has the organization identified those system components, services, or events that warrant logging according to the risk associated with the system and enable them on following systems: - Operating systems - Network Devices - Application - Firewall - VPN	FFIEC IS Booklet (2006) Appendix A: Objective 6 p. A6-A7 FFIEC IS Booklet (2006) Appendix A: Tier II: B, C, G, M p. A12-A15, A17, A22-A25	The examiner should review logging mechanisms in a similar manner as with physical systems. For AWS management activities, the examiner should review records for processes implemented to monitor service configuration changes. **Examiner should request and review** 1. The organizations Logging and Monitoring policies and procedures and their	Organization should define a processes to periodically monitor for service configuration changes. Just as physical systems, you must implement and maintain logging and monitoring of EC2 instances, applications deployed on EC2 instances, Amazon RDS databases, and any other services part of the client's EC2 environment.	The AWS Audit and Accountability Plan establishes a formally documented implementation plan and guidance for the acquisition, retention, and management of Amazon Web Services (AWS) log data. This is required to support several critical business processes, including service debugging, security incident investigation, and compliance activities. This plan also serves to interpret the requirements of the AWS Audit and Accounting Policy, which in turn should be used as a

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
			FFIEC AUD Booklet (2012) Appendix A: Tier II: D p. A13-A14	alignment/inclusion of AWS services		reference by teams when developing AWS service-specific log management procedures. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AU-1 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 10
LAM-2	Logging, Assessment Trails, and Monitoring	Has the organization implemented a centralized logging solution to store operating systems, servers and network devices logs in a central repository for a fixed period of time (approx. 90 days) to maintain assessment trails?	FFIEC IS Booklet (2006) Appendix A: Tier II: M p. A22-A25	The examiner should review logging mechanisms to ensure that they are configured to send logs to a centralized server in a similar manner as with physical systems. **Examiner should request and review** 1. The organizations Logging and Monitoring policies and procedures and their alignment/inclusion of AWS services: 2. AWS CloudTrail 3. AWS Config 4. S3 Server Logs	Although AWS logs and monitors access to the AWS console, they do not provide an interface for clients to monitor activity. Just as physical systems, organizations must implement and maintain logging and monitoring of EC2 instances, applications deployed on EC2 instances, Amazon RDS databases, and any other services part of the client's EC2 environment. Logs should be collected by a centralized logging solution for review and retention.	The AWS Audit and Accountability Plan establishes a formally documented implementation plan and guidance for the acquisition, retention, and management of Amazon Web Services (AWS) log data. This is required to support several critical business processes, including service debugging, security incident investigation, and compliance activities. This plan also serves to interpret the requirements of the AWS Audit and Accounting Policy. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AU-1 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 10
LAM-3	Logging, Assessment Trails, and Monitoring	Does the organization specify the type and format of logs to be retained?	FFIEC IS Booklet (2006) Appendix A: Tier II: M p. A22-A25	For Amazon EC2 instances, the examiner should review logging mechanisms to ensure that the proper types and formats of logs are retained in a similar manner as with physical systems. **Examiner should request and review** 1. The organizations Logging and Monitoring documentation related to logging formats to ensure the AWS log elements can be included	Although AWS logs and monitors access to the AWS console, they do not provide an interface for clients to monitor activity. Just as physical systems, organizations must implement and maintain logging and monitoring of EC2 instances, applications deployed on EC2 instances, Amazon RDS databases, and any other services part of the client's EC2 environment. The organization should determine the type and format of logs that will be retained.	The AWS Audit and Accountability Plan establishes a formally documented implementation plan and guidance for the acquisition, retention, and management of Amazon Web Services (AWS) log data. This is required to support several critical business processes, including service debugging, security incident investigation, and compliance activities. This plan also serves to interpret the requirements of the AWS Audit and Accounting Policy. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AU-1 SOC 2 – Section III, Area D

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
						PCI DSS v3.0 Requirement 10
LAM-4	Logging, Assessment Trails, and Monitoring	Does the organization have policies and procedures for the security of its log files? This includes: - Upholding segregation of duties and non-repudiation (system administrators should not be able to modify log contents) - Securing the transport of log files physically and logically - Delegating formal authority for log analysis	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: M p. A22-A25 FFIEC AUD Booklet (2012) Appendix A: Tier II: D p. A13-A15	The examiner should verify internal policies include AWS services and Amazon EC2 instances in relation to the oversight and monitoring of AWS log management capabilities. **Examiner should request and review** 1. The organizations Logging and Monitoring policies and procedures to ensure they address SoD, security and access authority	Although AWS logs and monitors access to the AWS console, they do not provide an interface for clients to monitor activity. Just as physical systems, organizations must implement and maintain logging and monitoring of EC2 instances, applications deployed on EC2 instances, Amazon RDS databases, and any other services part of the client's EC2 environment.	The AWS Audit and Accountability Plan establishes a formally documented implementation plan and guidance for the acquisition, retention, and management of Amazon Web Services (AWS) log data. This is required to support several critical business processes, including service debugging, security incident investigation, and compliance activities. This plan also serves to interpret the requirements of the AWS Audit and Accounting Policy. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AU-1 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 10
LAM-5	Logging, Assessment Trails, and Monitoring	The organization's network should be regularly monitored for problems (such as dropped packets, interference, or capacity problems) using network-monitoring tools.	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: B, M p. A12-A14, A22-A25	AWS also offers monitoring services, such as AWS CloudWatch and Describe API. If these are used, the examiner should review client process and records of their use for network monitoring. **Examiner should request and review** 1. Network logging implemented on Amazon EC2 instances and CloudWatch (in conjunction with AWS CloudTrail) use; if used within the organization	Clients do not have any network layer access within the AWS environment. AWS provides service performance monitoring services. Organization should evaluate the use of AWS CloudWatch: Amazon CloudWatch enables you to monitor your AWS resources in real-time, including Amazon EC2 instances, Amazon EBS volumes, Elastic Load Balancers, and Amazon RDS DB instances. Metrics such as CPU utilization, latency, and request counts are provided automatically for these AWS resources. Reference: CloudWatch	AWS Service Monitoring: Time Series Data (TSD) is Amazon's service-based monitoring solution and pipeline for aggregating and storing performance metrics Systems are configured to log these additional elements, and these events are captured in the auth.log / authpriv files of the systems. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: AU-2 & AU-3 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 11
Backup and Storage Controls						
BU-1	Backup and Storage Controls	Do the organization employ offsite data storage locations to recover data in the event of damage to the primary data facility?	FFIEC OPS Booklet (2004) Appendix A: Objective 6 p. A5-A6	The examiner should review use of AWS services for off-site backup and consider the appropriate controls from throughout this document as	AWS services may be used as a data backup facility. Developers and businesses around the globe rely on Amazon Web Services (AWS) for block	AWS stores user-level information using the EBS and S3 storage services available within AWS. When data is stored in EBS or S3 redundant copies are automatically and synchronously

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
			FFIEC OPS Booklet (2004) Appendix A: Tier II: C p. A12-A13	appropriate for the data being stored in AWS. **Examiner should request and review** 1. The organizations back-up and storage policies and procedures and evaluate how AWS is used within their backup strategy	storage, file storage, backup, archive, and disaster recovery. Organizations should evaluate and document how they uses AWS within their back-up and storage strategies. References: AWS Backup/Storage	created whenever the data is changed and the copies are validated to be identical to the original data. AWS maintains the durability of the data by automatically detecting and repairing any lost redundancy. If corruption is detected, it is automatically repaired using redundant data to ensure the integrity of the data. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-09 SOC 2 – Section III, Area C
BU-2	Backup and Storage Controls	Does management maintain inventories of all backup media stored at offsite locations? Frequent inventories checks should be performed to ensure the availability of all backup media.	FFIEC OPS Booklet (2004) Appendix A: Objective 6 p. A5-A6	The examiner should review inventory of data backed up to AWS services as off-site backup. **Examiner should request and review:** 1. The organizations back-up and storage policies and procedures for identifications of offsite storage locations and/or use of AWS for offsite storage	AWS services may be used as a data backup facility. Developers and businesses around the globe rely on Amazon Web Services (AWS) for block storage, file storage, backup, archive, and disaster recovery. Organizations should evaluate and document how they uses AWS within their back-up and storage strategies.	AWS automatically and synchronously storing data whenever the data is changed across both multiple devices and multiple facilities within a selected geographical Region, S3 storage provides the highest level of data durability and availability in the AWS IaaS. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-09 SOC 2 – Section III, Area C
BU-3	Backup and Storage Controls	Are backup and storage controls scalable to allow for future growth?	FFIEC OPS Booklet (2004) Appendix A: Objective 6 p. A5-A6	The examiner should review plan for projected data backup requirements and current use of AWS services to support this growth. **Examiner should request and review:** 1. The organizations back-up and storage policies and procedures for scalability and use of AWS services	AWS services may be used as a data backup facility. AWS maintains data in audited data centers and does not use removable media. Clients are responsible for planning and budgeting future AWS use. The use of AWS allows for a scalable solution to allow for future growth.	Data is stored in AWS redundant copies are automatically created and are validated to be identical to the original data. AWS maintains the durability of the data by automatically detecting and repairing any lost redundancy. If corruption is detected, it is automatically repaired using redundant data to ensure the integrity of the data. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-09 SOC 2 – Section III, Area C

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
BU-4	Backup and Storage Controls	Is backup media protected (physical and encryption) to prevent unauthorized access to sensitive data?	FFIEC OPS Booklet (2004) Appendix A: Objective 6 p. A5-A6	The examiner should review inventory of data backed up to AWS services as off-site backup. AWS does not use removable media. **Examiner should request and review:** 1. The organizations back-up and storage policies and procedures to better understand the protection in place to protect data internally and within AWS	AWS services may be used as a data backup facility. AWS maintains data in audited data centers and does not use removable media. Although AWS does not use any removable backup media, for additional protection of the data the client may Use either server-side encryption where supported or encrypt data before storing with AWS services and Ensure that keys are maintained in a secure manner to help protect the data.	AWS protects the confidentiality of transmitted data through the use of symmetric encryption of data before transmission to ensure the message contents are not readable in transit. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SC—09 SOC 2 – Section III, Area C
BU-5	Backup and Storage Controls	Are regular tests performed on offsite data media to ensure the operability of the media as required?	FFIEC BCP Booklet (2008) Appendix A: Objective 6 p. A8 FFIEC OPS Booklet (2004) Appendix A: Objective 6 p. A5-A6	The examiner should review records of testing backup data stored in AWS services. **Examiner should request and review:** 1. The organizations back-up and storage policies and procedures to validate the organizations testing processes	AWS services may be used as a data backup facility. AWS maintains data in audited data centers and does not use removable media. The organization should conduct regular restore testing as it would with any backup service as it would with any other backup service provider.	Data is stored in AWS redundant copies are automatically created and are validated to be identical to the original data. AWS maintains the durability of the data by automatically detecting and repairing any lost redundancy. If corruption is detected, it is automatically repaired using redundant data to ensure the integrity of the data. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: CP-09
Encryption Controls						
ENC-1	Encryption Controls	Are there appropriate controls in place to protect confidential client information while in transport (e.g., transport encryption, certificates, and secure file shares) and storage?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: L p. A21-A22 FFIEC OPS Booklet (2004)	The examiner should review methods for connecting to AWS Console, management API, S3, RDS, and Amazon EC2 VPN. The examiner should consider the controls implemented for management access as well as reviewing application controls that may be deployed on the systems hosted in AWS. **Examiner should request and review:**	AWS provides features for transmission and storage encryption, including HTTPS for Console and web service interface and server-side encryption for storage. EC2 instances are completely under the control of the client. Clients are responsible for implementation and management of encryption that may be implemented and used on EC2 resources.	For storage, the AWS Acceptable Encryption Standard spells out approved methods for credential and key storage. These include: ▪ AWS Key Management Service ▪ Window DPAPI ▪ MAC OS X Keychain ▪ Password Safe ▪ AWS CloudHSM Hardware Security Modules **Reference**: NIST SP 800-53 rev.3

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
			Appendix A: Objective 5 p. A4-A5	1. Policies and procedures related to data protections at rest, transmit and use both internally and within AWS services	Organization should understand and evaluate the security capabilities within AWS. Reference: AWS Security Resources	FedRAMP Control: IA-05 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 4
ENC-2	Encryption Controls	Encryption algorithms employed to protect data should be strong enough to protect data until disclosure poses no material risk.	FFIEC IS Booklet (2006) Appendix A: Tier II: K, L p. A20-A22	The examiner should review methods for connecting to AWS Console, management API, and Amazon EC2 VPN for enforcement of encryption. **Examiner should request and review:** 1. Encryption processes used to protect data on Amazon EC2 instances similar to physical systems 2. Configuration of AWS Key Management Service, including integration with Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, and Amazon Elastic Transcoder 3. Configuration of AWS CloudHSM	AWS provides features for transmission and storage encryption, including HTTPS for Console and web service interface, and server-side encryption for storage. EC2 instances are completely under the control of the client. Clients are responsible for implementation and management of encryption by EC2 resources.	AWS uses multiple algorithms and cyphers such as Open SSL utilizes SSL/TLS and cryptographic ciphers including AES and 3DES Ciphers for encryption of transmitted data, x.509 server certificate with RSA keys for server authenticity and Cryptographic ciphers including SHA-1 for message integrity **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IA-07 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 3 & 4
ENC-3	Encryption Controls	Does the organization implement encryption on the transport and storage of all authentication credentials?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: K p. A20-A21	The examiner should review methods for connecting to AWS Console, management API, and Amazon EC2 VPN for enforcement of encryption. **Examiner should request and review:** 1. Encryption processes used to protect data on Amazon EC2 instances similar to physical systems	AWS provides features for transmission and storage encryption, including HTTPS for Console and web service interface and server-side encryption for storage. EC2 instances are completely under the control of the client. Clients are responsible for implementation and management of encryption by EC2 resources.	AWS uses multiple algorithms and cyphers such as Open SSL utilizes SSL/TLS and cryptographic ciphers including AES and 3DES Ciphers for encryption of transmitted data, x.509 server certificate with RSA keys for server authenticity and Cryptographic ciphers including SHA-1 for message integrity **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IA-07 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 8
ENC-4	Encryption Controls	Does the organization have an encryption key management	FFIEC IS Booklet (2006)	The examiner should review internal policies and procedures for key	AWS provides features supporting key management. Clients are responsible	AWS produces, controls, and distributes symmetric cryptographic

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		policy? Encryption keys should be treated as confidential information and protected with layered administrative and technical controls. Good key security practices include: key rotation, unique key generation, documenting key distribution and revocation, destroying potentially compromised keys, instantiating key activation and deactivation timeframes.	Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: K p. A20-A21	management include AWS services and Amazon EC2 instances. **Examiner should request and review:** 1. The key management processes on Amazon EC2 instances in a similar manner as with physical systems	for implementing encryption key management. EC2 instances are completely under the control of the client. Clients are responsible for implementation and management of encryption keys by EC2 resources. Clients have the option to leverage several technologies such as CloudHSM to manage keys for systems that are hosted in AWS to provide a hardware-based solution for key management that is solely under the control of the client.	keys using NIST approved key management technology and processes in the AWS information system. AWS developed a secure key and credential manager and is the primary system used to create, protect and distribute symmetric keys at AWS. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SC-12 PCI DSS v3.0 Requirement 3
Malicious Code Controls						
MC-1	Malicious Code Controls	Is Antivirus and anti-spyware software deployed on all critical servers and workstations?	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: B, C, D p. A12-A16	The examiner should review anti-malware on Amazon EC2 instances in a similar manner as with physical systems. **Examiner should request and review:** 1. Policies and procedures related to Antivirus and valid it includes AWS services. .	EC2 instances are completely under the control of the client. Clients are responsible for implementation and management of anti-malware for EC2 resources. Reference: • AWS & Symantec • AWS & Trend Micro	AWS Security has defined, but has not limited its denial of service protection ability to the following types of denial of service attacks: • Flooding attacks - receiving a very large number of well-formed API calls with bad signatures; high rate packet flooding • Software / logic attacks - application level attacks • Distributed attacks - flooding attacks from multiple locations • Unintentional denial of service - enormous spike in usage **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SC-05 SOC 2, Section IV PCI DSS v3.0 Requirement 5
MC-2	Malicious Code Controls	Are antivirus and anti-spyware signatures and updates consistently deployed as	FFIEC IS Booklet (2006)	The examiner should review anti-malware on Amazon EC2 instances in a	EC2 instances are completely under the control of the client. Clients are responsible for implementation and	AWS Security has defined, but has not limited its denial of service protection

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		released? Are logs of AV patches and updates maintained?	Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: B, C, D p. A12-A16	similar manner as with physical systems. **Examiner should request and review:** 1. Policies and procedures related to Antivirus and valid it includes AWS services.	management of anti-malware for EC2 resources.	ability to the following types of denial of service attacks: • Flooding attacks - receiving a very large number of well-formed API calls with bad signatures; high rate packet flooding • Software / logic attacks - application level attacks • Distributed attacks - flooding attacks from multiple locations • Unintentional denial of service - enormous spike in usage **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SC-05 SOC 2 – Section IV PCI DSS v3.0 Requirement 5
MC-3	Malicious Code Controls	Perimeter security tools (including intrusion detection and prevention systems, and application firewalls) should block malicious code before entry into the internal network.	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should review anti-malware on Amazon EC2 instances in a similar manner as with physical systems. **Examiner should request and review:** 1. Policies and procedures related to intrusion detection and valid it includes AWS services.	Clients do not have access to AWS networks. However, EC2 instances can be implemented as logical network segmentation within the client's EC2 environment.	AWS Security has defined, but has not limited its denial of service protection ability to the following types of denial of service attacks: • Flooding attacks - receiving a very large number of well-formed API calls with bad signatures; high rate packet flooding • Software / logic attacks - application level attacks • Distributed attacks - flooding attacks from multiple locations • Unintentional denial of service - enormous spike in usage **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SC-05 SOC 2 – Section IV PCI DSS v3.0 Requirement 1 & 6

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
Intrusion Detection and Response						
IDS-1	Intrusion Detection and Response	Has the organization deployed intrusion detection systems to monitor unauthorized access to client information systems?	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14	The examiner should review host-based IDS on Amazon EC2 instances in a similar manner as with physical systems. See AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for the network. **Examiner should request and review:** 1. The organizations policies and procedures related to IDS and the implementation of IDS within the use of AWS services.	Clients do not have access to AWS networks. However, host-based intrusion detection can be implemented on EC2 instances. Reference: Security Resources	AWS uses a monitoring tool for gauging performance metrics and trends. In doing so, the Security and Service team owners leverage collected statistics to evaluate anomalies in system behavior. The system incorporates a monitoring agent that runs on targeted hosts to collect metrics and to evaluate the metrics against alarm specifications. Metrics are available via an online console, which is available to all Amazon service owners for viewing current status and future analysis. Alarms can also be configured to issue trouble-tickets or email notifications. Host-based metrics are provided at 1-minute intervals. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IR-04 SOC 2 – Section IV PCI DSS v3.0 Requirement 11
IDS-2	Intrusion Detection and Response	Intrusion detection devices should be used to monitor all actions performed on the firewall and all traffic allowed through the firewall.	FFIEC IS Booklet (2006) Appendix A: Tier II: M p. A22-A25	AWS manages all networks for AWS services. **Examiner should request and review:** 1. AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed.	Clients do not have access to AWS networks. Management of AWS Security Groups can be monitored via the AWS API.	AWS monitors all network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the system and at key internal boundaries within the system. **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: SC-07 SOC 2 – Section IV PCI DSS v3.0 Requirement 11
IDS-3	Intrusion Detection and Response	Are IDS/IPS logs stored and monitored to detect any intrusion attempts?	FFIEC AUD Booklet (2012) Appendix A: Tier II: D	Amazon CloudWatch enables organization to monitor your AWS resources in real-time, including Amazon EC2 instances, Amazon EBS	Clients do not have access to AWS networks. However, host-based intrusion detection can be implemented on EC2 instances.	For storage, the AWS Acceptable Encryption Standard spells out approved methods for credential and key storage. These include:

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
			p. A13-A15	volumes, Elastic Load Balancers, and Amazon RDS DB instances. **Examiner should request and review:** 1. The organizations use and configuration of CloudWatch and how logs are stored and protected.	Similarly, clients are responsible for implementation of logging within their EC2 environment.	▪ Odin - an AWS developed secure key and credential manager ▪ Window DPAPI ▪ MAC OS X Keychain ▪ Password Safe ▪ Thales nShield Hardware Security Modules **Reference**: NIST SP 800-53 rev.3 FedRAMP Control: IA-05 SOC 2 – Section IV PCI DSS v3.0 Requirement 10
Documentation and Inventory						
DI-1	Documentation and Inventory	The network is fully documented, including remote and public access, with documentation available only to authorized persons.	FFIEC IS Booklet (2006) Appendix A: Tier II: B p. A12-A14 FFIEC OPS Booklet (2004) Appendix A: Objective 4 p. A3-A4	The examiner should verify that AWS services and Direct Connect and VPN connections are included in inventory documentation. **Examiner should request and review:** AWS Config reports for AWS resource inventory, configuration history, and configuration change notifications.	**Audit Guidance:** Provide system inventory and documentation for all relevant systems and AWS services. **Implementation Guidance:** In addition to inventory and documentation of physical systems, clients should maintain an inventory and documentation for all AWS resources and their management process for AWS services.	**Reference:** SOC 2 – Section IV PCI DSS v3.0 Requirement 1
DI-2	Documentation and Inventory	Is an inventory of all critical systems maintained and updated as necessary?	FFIEC OPS Booklet (2004) Appendix A: Tier II: A p. A11-A12	The examiner should verify that Amazon EC2 instances are included in inventory documentation. **Examiner should request and review:** AWS Config reports for AWS resource inventory, configuration history, and configuration change notifications.	**Audit Guidance:** Provide system inventory and documentation for all relevant systems and AWS services. **Implementation Guidance:** In addition to inventory and documentation of physical systems, clients should maintain an inventory and documentation for all AWS resources and their management process for AWS services.	AWS uses a configuration management tool to manage deployable software in packages, package groups, and environments. The package service is a collection of related files, such as software, content, etc., that are tightly coupled to one another. A package group is a set of packages that are often deployed together. **Reference:** SOC 2 – Section IV PCI DSS v3.0 Requirement 2
DI-3	Documentation and Inventory	Is there an information classification program appropriate to the complexity of	FFIEC IS Booklet (2006)	The examiner should verify that that information classification policy and	**Audit Guidance:** Provide information classification program description.	The AWS Data Handling Standard defines AWS client information as

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		its systems where information is classified according to its sensitivity and importance for meeting business objectives? Controls commensurate to the sensitivity and importance should be based on these classifications. Media handling and disposition policies should reflect the overall classification strategy.	Appendix A: Tier II: L p. A21-A22 FFIEC OPS Booklet (2004) Appendix A: Objective 5 p. A4-A5	processes include AWS services and Amazon EC2 instances.	**Implementation Guidance:** AWS services and management should be included within the scope of systems and media governed by information classification policies and processes.	critical information. The AWS data handling requirements set forth in the standard require that AWS critical information be encrypted in transit and at rest, and defines requirements for access, access control, access logging and physical control. **Reference:** SOC 2 – Appendix I PCI DSS v3.0 Requirement 12
Physical						
PS-1	Physical Security Controls	Does the organization implement defined physical security zones (Facility, data center, sensitive work areas, and workstations) and implement appropriate preventive and detective controls in each zone. The security zones should: - Prevent physical penetration by unauthorized individuals. - Ensure protection against environmental contaminants - Ensure protection against Tempest attacks, rogue wireless access points, and electromagnetic interference.	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet (2006) Appendix A: Tier II: E p. A16 FFIEC OPS Booklet (2004) Appendix A: Tier II: E p. A13-A14	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	AWS has implemented a formal, documented physical and environmental protection policy called "AWS Physical and Environmental Protection Policy,". Additional details can be reviewed by requesting our certifications & reports **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-2	Physical Security Controls	Is the datacenter protected from external intruders by sufficient deterrent controls such as: - Secure Doors and windows to the datacenter - The datacenter should not be designated by signage or readily identifiable to external sources. - The datacenter should be protected by sufficient detective controls, such as: physical	FFIEC IS Booklet (2006) Appendix A: Tier II: E p. A16 FFIEC OPS Booklet (2004) Appendix A: Tier II: E p. A13-A14	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	Physical access to all AWS data centers, collocations, and POP facilities housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access in order to execute their jobs. Additional details can be reviewed by requesting our certifications & reports

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		intrusion detection systems, alarms, motion detectors, CCTV, and other surveillance systems - The network operations center should be considered as sensitive location and have restricted physical access to only authorized individuals				**Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-3	Physical Security Controls	Raised floors, fire suppression systems, smoke alarm anti-static flooring, etc. should mitigate environmental risks.	FFIEC IS Booklet (2006) Appendix A: Tier II: E p. A16 FFIEC OPS Booklet (2004) Appendix A: Objective 7 p. A6 FFIEC OPS Booklet (2004) Appendix A: Tier II: D p. A13	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	AWS Data Centers are Tier III data center facilities, and have implemented an N+1 redundancy architecture to ensure system availability in the event of a component failure. Additional details can be reviewed by requesting our certifications & reports **Reference:** SOC 2 – Section III, Area C
PS-4	Physical Security Controls	Employees who access secure areas should display proper identification and be authorized for access.	FFIEC IS Booklet (2006) Appendix A: Tier II: E p. A16 FFIEC OPS Booklet (2004) Appendix A: Tier II: E p. A13-A14	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	Authorization credentials, which include an electronic access badge (unique to the employee, vendor or contractor) and PIN—are provided to authorized personnel in order to physically access the data center facilities. Additional details can be reviewed by requesting our certifications & reports **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
PS-5	Physical Security Controls	All visitors accessing non-public areas should wear proper identification.	FFIEC OPS Booklet (2004) Appendix A: Tier II: E p. A13-A14	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	AWS only provides data center access and information to vendors, contractors, and visitors who have a legitimate business need for such privileges, such as emergency repairs or data center tours under certain, limited circumstances. Additional details can be reviewed by requesting our certifications & reports **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-6	Physical Security Controls	Is visitor access logged, and if so is this log maintained for a period of at least 30 days.	FFIEC AUD Booklet (2012) Appendix A: Tier II: D A13-A14	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	The Vice President of AWS Utility Computing Services must approve all visitor requests. This request must contain a complete list of all personnel to be included in the tour group as well as justification for the tour request and how it will be beneficial for the recipients. A copy of this approved communication is included as an attachment to the AWS Ticketing System ticket, prior to approval for access to the data center. **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-7	Physical Security Controls	Formal procedures should exist for any and all transfers of hardware and software from the organization's premises.	FFIEC OPS Booklet (2004) Appendix A: Tier II: E p. A13-A14	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	All information system components, such as servers, racks, network devices, hard drives, system hardware components, and building materials that are shipped to and received by data centers within the system boundary require prior authorization by and notification to the Data Center Manager.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
						The Infrastructure Automation tool is used for Service Owners to manage fleets, hardware, and provision metrics such as rack acquisition efficiency. **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-8	Physical Security Controls	All telecommunications equipment such as network devices, Network cabling and wiring should be considered a sensitive location and have restricted physical access to only authorized individuals.	FFIEC OPS Booklet (2004) Appendix A: Objective 8 p. A7-A8 FFIEC OPS Booklet (2004) Appendix A: Tier II: D p. A13	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	AWS utilizes multi-factor authentication mechanisms for data center access as well as additional security mechanisms to ensure that only authorized individuals enter an AWS data center. Authorized employees/contractors must use their designated badge on the card reader and enter their unique digit PIN to gain access to the facility and rooms for which they are authorized. **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-9	Physical Security Controls	Network cabling and wiring should be well documented and physically organized to facilitate maintenance, repair, and upgrades.	FFIEC OPS Booklet (2004) Appendix A: Objective 8 p. A7-A8	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	Transmission lines within buildings, both hidden and visible, as well as the cables outside of buildings are protected from accidental damage, disruption, and physical tampering by the use of secure conduit. **Reference:** SOC 2 – Section III, Area C
PS-10	Physical Security Controls	The organization should ensure that all terminals providing operating system access are located in physically secure and monitored environments.	FFIEC IS Booklet (2006) Appendix A: Objective 4 p. A4-A5	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	Systems, which can be plugged into servers—are the only output devices used within data centers. These systems reside only within data center server rooms, which are protected by physical access devices (badge readers) requiring a successful badge swipe and PIN to enter.

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
						Reference: SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-11	Physical Security Controls	Do PCs or workstations employ screensaver passwords or automatic session timeouts to prevent unauthorized use?	FFIEC IS Booklet (2006) Appendix A: Tier II: D p. A15-A16	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	AWS has implemented a formal, documented identification and authentication policy, which is applicable to AWS, titled "AWS Identification and Authentication Policy". Which includes session timeouts. **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 8
PS-12	Physical Security Controls	The facility's external perimeter should have adequate deterrent and detective controls, such as sufficient lighting, fences, guards, video surveillance, and alarms.	FFIEC OPS Booklet (2004) Appendix A: Tier II: E p. A13-A14	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	AWS Data Centers are Tier III data center facilities, and have implemented an N+1 redundancy architecture to ensure system availability in the event of a component failure. As such, components (N) have at least one independent backup component (+1). **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-13	Physical Security Controls	Management should employ a fixed-asset tracking system to inventory all critical and valuable equipment.	FFIEC OPS Booklet (2004) Appendix A: Tier II: A p. A11-A12	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	All information system components, which include, but are not limited to, servers, racks, network devices, hard drives, system hardware components, and building materials that are shipped to and received by data centers within the system boundary require prior authorization by and notification to the Data Center Manager. **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 2
PS-14	Physical Security Controls	Does management implement media disposition policies and procedures that address the destruction of confidential paper documents and the	FFIEC IS Booklet (2006) Appendix A: Tier II: D p. A15-A16	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	AWS sanitizes all forms of digital media, regardless if it is removable storage or non-removable storage. AWS does not sanitize non-digital media, as the AWS

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
		sterilization of electronic media prior to disposal?	FFIEC OPS Booklet (2004) Appendix A: Objective 5 p. A4-A5			system does not provide services that render printed media. **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-15	Physical Security Controls	Does management maintain a policy for mobile computer and removable media to prevent transfer of sensitive data?	FFIEC OPS Booklet (2004) Appendix A: Tier II: E p. A13-A14	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	Magnetic, non-magnetic, and hardcopy media types are not used to store data, so are not transported outside of the AWS service boundaries. **Reference:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 12
Environmental						
EC-1	Environmental Controls	Computing equipment (particularly critical systems) should have an uninterruptible power supply (UPS).	FFIEC OPS Booklet (2004) Appendix A: Objective 7 p. A6 FFIEC OPS Booklet (2004) Appendix A: Tier II: D p. A13	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	AWS Data Centers are Tier III data center facilities, and have implemented an N+1 redundancy architecture to ensure system availability in the event of a component failure. As such, components (N) have at least one independent backup component (+1). AWS employs N+1 redundancy with active-active components, so the backup component is active in the operation even when all other components are fully functional. **Reference:** SOC 2 – Section III, Area C
EC-2	Environmental Controls	Fuel-powered backup systems should have sufficient fuel on hand to power operations for at least two to three days.	FFIEC OPS Booklet (2004) Appendix A: Objective 7 p. A6 FFIEC OPS Booklet (2004) Appendix A: Tier II: D p. A13	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	AWS Data Centers are Tier III data center facilities, and have implemented an N+1 redundancy architecture to ensure system availability in the event of a component failure. As such, components (N) have at least one independent backup component (+1). AWS employs N+1 redundancy with active-active components, so the backup component is active in the operation even when all other components are fully functional. **Reference:** SOC 2 – Section III, Area C

Control	Control Area	Control Objective	Control Reference	Examiner Guidance	Client Guidance	AWS Evidence
EC-3	Environmental Controls	Operations centers should have adequate heating, ventilation, and air conditioning (HVAC) solutions in order for personnel and technology to function properly.	FFIEC OPS Booklet (2004) Appendix A: Objective 7 p. A6 FFIEC OPS Booklet (2004) Appendix A: Tier II: D p. A13	The examiner should review the AWS Provided Evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.	AWS is responsible for physical controls.	Temperature and humidity levels of data center server and network rooms are maintained and managed at levels established by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE). **Reference:** SOC 2 – Section III, Area C