U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE)

CYBERSECURITY INITIATIVE
Workbook

Notices

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

Table of Contents

Executive Summary

The Amazon Web Services (AWS) cloud environment is designed with security in mind and may be utilized by customers to satisfy a wide range of regulatory requirements, including those imposed by the U.S. Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE). This document provides an overview of the OCIE Cybersecurity initiative, AWS relevant Service Provider features and controls, and illustrates the OCIE's Cybersecurity Initiative compliance responsibilities for customer's use of AWS. Services may require specific configurations, connectivity and architecture considerations for use within an SEC compliant manner.

The document is to be used by AWS securities industry customers, their examiners, and advisors to understand the scope of the AWS services, guidance for implementation, and examination when using AWS as part of the financial institutions environment.

OCIE's Cybersecurity Initiative Overview

As you may be aware, on April 15, 2014, the SEC issued a National Exam Program Risk Alert entitled OCIE Cybersecurity Initiative. This came at the heels of the SEC sponsored Cybersecurity Roundtable which underscored the importance of the integrity of the U.S. market system and customer data protection; as well as the compelling need for stronger partnerships between the government and private sector to address cyber threats and consider what additional steps the SEC should take to address cyber-threats.

The OCIE's Cybersecurity Initiative was designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats. The focus of the Initiative is on the broker-dealers and registered investment advisers within the following security domains:

- Cybersecurity governance,
- Identification and assessment of cybersecurity risks (Risk Assessments),
- Protection of networks and information,
- Risks associated with remote customer access and funds transfer requests,
- Risks associated with vendors and other third parties,
- Detection of unauthorized activity, and
- Experiences with certain cybersecurity threats.

Description of In-Scope Services

AWS Management Environment is the underlying physical and logical infrastructure that supports 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 OCIE controls review:

- Amazon Elastic Block Storage (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Identity and Access Management (IAM)
- Amazon Simple Storage Service (S3)
- Amazon Virtual Private Cloud (VPC)

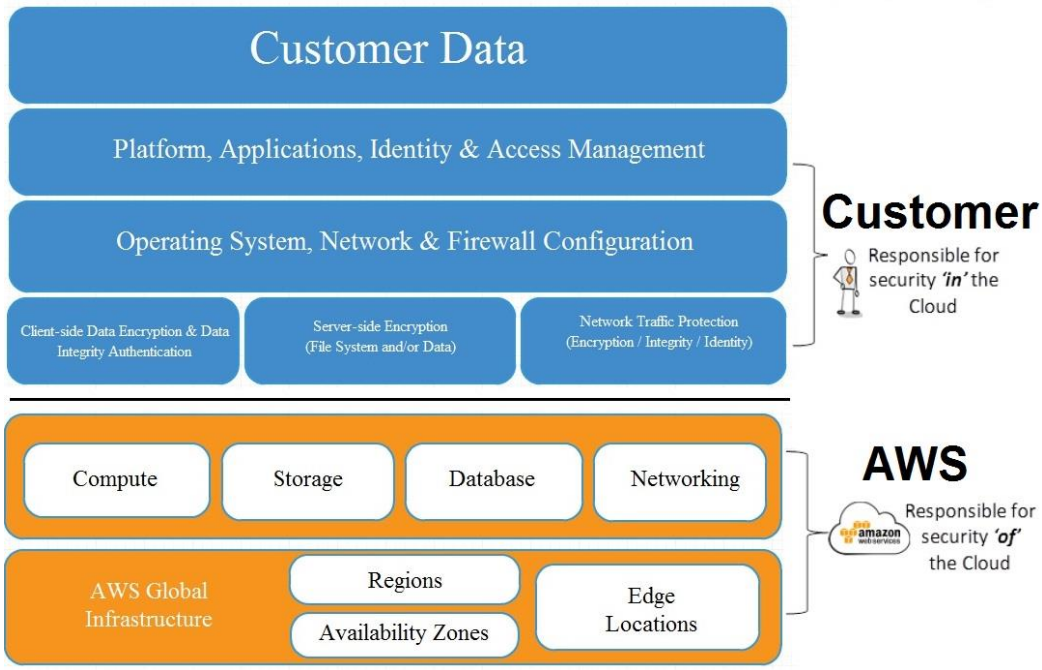
For broader descriptions of each service see the [AWS Products website]

AWS Shared Responsibility Model

As with any third parties, utilizing AWS creates 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 you operate, manage and control components of information security controls. Security controls are considered to be shared, inherited, or dual controls. In terms of information security and compliance in cloud computing there is a subtle but very important distinction in understanding and evaluating compliance of the cloud solution and understanding and evaluating your usage of the cloud solution.

"Security and Compliance *OF* the cloud" pertains to the security programs and measures which the Cloud Service Provider (AWS) implements within the AWS Infrastructure; "Security and Compliance *IN* the cloud" relates to the implementation of security controls associated with workloads running on top of the AWS infrastructure.

Shared Responsibility Model Illustrated



Regions, Availability Zones, and Endpoints

You should also be familiar with regions, Availability Zones, and endpoints, which are components of the AWS secure global infrastructure. 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.

You are responsible for carefully selecting the Availability Zones where your systems will reside. 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.

Simplifying the Compliance Process

In order to manage risk and security within the cloud, a variety of processes and guidelines have been created to differentiate between the compliance of a cloud service provider and the responsibilities of a subscriber consuming the cloud services. One of the primary concepts that have emerged is the increased understanding and documentation of shared, inherited or dual (AWS & Customer) controls in a cloud environment.

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, reviewing compliance of workloads running on top of the AWS infrastructure gives an idea of "Security & compliance ***IN*** the cloud".

Security & Compliance *OF* the Cloud

In order to manage risk and security within the cloud, a variety of processes and guidelines have been created to differentiate between the security of a cloud service provider and the responsibilities of a customer consuming the cloud services. One of the primary concepts that have emerged is the increased understanding and documentation of shared, inherited or dual (AWS & Customer) security controls in a cloud environment. 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 security controls that are met by approaching the AWS Cloud in two distinct ways: first, reviewing compliance of the AWS Infrastructure gives an idea of "Security & Compliance *OF* the cloud"; and second, reviewing the security of workloads running on top of the AWS infrastructure gives an idea of "Security & Compliance *IN* the cloud". 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. Customers running workloads on the AWS infrastructure depend on AWS for a number of security controls. AWS has several additional whitepapers, which provide additional information to assist AWS customers with integrating AWS into their existing security frameworks and to help design and execute security assessments of an organization's use of AWS. See: AWS Compliance Whitepapers

Security & Compliance *IN* the Cloud

Security & Compliance *IN* the Cloud refers to how the customer manages the security of their workloads through the use of (virtual private clouds, security groups, operating systems, data bases, authentication, etc.)

Cross-service security controls – Are security controls, which a customer needs to implement across all services within their AWS customer instance. While each customer's use of AWS services may vary along with their own risk posture and security control interpretation, cross service controls will need to be documented within the customer's use of AWS services.

> **Example:** Multi-factor authentication can be used to help secure Identity and Access Management (IAM) users, groups and roles within the customer environment in-order to meet SEC Access Management, Authentication, and Authorization requirements for an educational agency, institutions and/or service organization

Service-Specific security controls – Are service specific security implementation such as the Amazon Simple Storage Service (S3) security access permission settings, logging, event notification and/or encryption. A customer may need to document service specific controls within their use of S3 in-order to meet a specific security control objective related to student records, PII and/or directory services related to education records.

> **Example**: Server Side Encryption (SSE) is enabled for all objects classified as student records, educational and/or directory information related to the SEC information.

Optimized Network, Operating Systems (OS) and Application Controls – Controls a customer may need to document in-order to meet specific control elements related to the use an Operating Systems and/or application deployed within in AWS.

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

Scope of Guidance

The AWS service architecture relevant to an OCIE compliant environment includes those services listed in the "Description of In-Scope Environment" section of this document, including the underlying physical and logical infrastructure. The technology used to administer and deliver these services to AWS customers is explained in more detail below. This service architecture is audited globally for relevant controls primarily under the Service Organization Controls reporting standard and attested to by a Certified Public Account firm.

AWS Management Environment

AWS's world-class, highly secure data centers utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. And multiple geographic regions and Availability Zones allow you to remain resilient in the face of most failure modes, including natural disasters or system failures.

Physical and Environmental Security

AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

Secure Network Architecture

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.

Secure Access Points

AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet service providers (ISPs). AWS employs a redundant connection to more than one communication service at each Internet-facing edge of the AWS network. These connections each have dedicated network devices.

Network Monitoring and Protection

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

Visit the AWS Security Center for more frequently asked questions about compliance and for the AWS Security Whitepaper.

Commission's Office of Compliance Inspections and Examinations (OCIE)

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

Section 1	Cybersecurity Governance/Identification of Risks		
For each of the following practices employed by the Firm for management of information security assets please provide the month and year in which the noted action was last taken Please also provide a copy of any relevant policies and procedures:			
Question No.	**Requirement**	**Responsibility**	**AWS Supporting Details**
1	For each of the following practices employed by the Firm for management of information security assets please provide the month and year in which the noted action was last taken Please also provide a copy of any relevant policies and procedures.		
1.1	Physical devices and systems within the Firm are inventoried.	Shared	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: • Version control - all updates are version controlled and previous version are available as needed • Access control - the user making the changes has permission to do so and changes are associated with a specific user • Documentation - the purpose of the change is captured Reference: NIST SP 800-53 rev.3 FedRAMP Control: CM-2

Question No.	Requirement	Responsibility	AWS Supporting Details
1.2	Software platforms and applications within the Firm are inventoried.	Shared	Software configurations implemented to systems and devices within AWS are stored and implemented by the respective Service and Infrastructure teams. AWS service teams employ automated mechanisms to centrally manage, apply, and verify configuration settings. Reference: NIST SP 800-53 rev.3 FedRAMP Control: CM-2
1.3	Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated.	Customer Specific	
1.4	Connections to the Firm's network from external sources are catalogued.	Customer Specific	
1.5	Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value.	Shared	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
1.6	Logging capabilities and practices are assessed for adequacy, appropriate retention, and secure maintenance.	Shared	The AWS Audit and Accountability Plan establish 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 reference by teams when developing AWS service-specific log management procedures. Reference: NIST SP 800-53 rev.3 FedRAMP Control: AU-1

Question No.	Requirement	Responsibility	AWS Supporting Details
2	Copy of the Firm's written information security policy.	Shared	AWS has implemented a formal information security program designed to protect the confidentiality, integrity, and availability of customers' 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
3	Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. If such assessments are conducted: • Who (business group/title) conducts them, and in what month and year was the most recent assessment completed? • Please describe any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated.	Shared	An annual risk assessment which covers all AWS regions and business 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 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

Question No.	Requirement	Responsibility	AWS Supporting Details
4	Please indicate whether the Firm conducts periodic risk assessments to identify physical security threats and vulnerabilities that may bear on cybersecurity. If such assessments are conducted: • Who (business group/title) conducts them, and in what month and year was the most recent assessment completed? • Please describe any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated.	Shared	An annual risk assessment which covers all AWS regions and business 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 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
5	If cybersecurity roles and responsibilities for the Firm's workforce and managers have been explicitly assigned and communicated, please provide written documentation of these roles and responsibilities. If no written documentation exists, please provide a brief description.	Shared	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.6.1.2
6	Please provide a copy of the Firm's written business continuity of operations plan that addresses mitigation of the effects of a cybersecurity incident and/or recovery from such an incident if one exists. 1. As well as the nature of the resolution of those claims.	Shared	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

Question No.	Requirement	Responsibility	AWS Supporting Details
7	Does the Firm have a Chief Information Security Officer or equivalent position? If so, please identify the person and title. If not, where does principal responsibility for overseeing cybersecurity reside within the Firm?	Shared	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.6.1.2
8	Does the Firm maintain insurance that specifically covers losses and expenses attributable to cybersecurity incidents? If so, please briefly describe the nature of the coverage and indicate whether the Firm has filed any claims, as	Customer Specific	
Section 2	**Protection of Firm Networks and Information**		
Question No.	**Requirement**	**Responsibility**	**AWS Supporting Details**
9	Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), the Firm has used to model its information security architecture and processes.	Shared	AWS has used the following best practices and frameworks to model its information security architecture and processes: SOC 1, SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FedRAMP, HIPAA, and Australian Signals Directorate ISM

Question No.	Requirement	Responsibility	AWS Supporting Details
10	Please indicate which of the following practices and controls regarding the protection of its networks and information are utilized by the Firm, and provide any relevant policies and procedures for each item.		
10.1	The Firm provides written guidance and periodic training to employees concerning information security risks and responsibilities. If the Firm provides such guidance and/or training, please provide a copy of any related written materials (e.g., presentations) and identify the dates, topics, and which groups of employees participated in each training event conducted since January 1, 2013.	Shared	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
10.2	The Firm maintains controls to prevent unauthorized escalation of user privileges and lateral movement among network resources. If so, please describe the controls, unless fully described within policies and procedures.	Shared	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. Reference: NIST SP 800-53 rev.3 FedRAMP Control: AC-1

Question No.	Requirement	Responsibility	AWS Supporting Details
10.3	The Firm restricts users to those network resources necessary for their business functions. If so, please describe those controls, unless fully described within policies and procedures.	Shared	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). 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
10.4	The Firm maintains an environment for testing and development of software and applications that is separate from its business environment.	Shared	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
10.5	The Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorization and an assessment of security implications.	Shared	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. Reference: NIST SP 800-53 rev.3 FedRAMP Control: CM-1

Question No.	Requirement	Responsibility	AWS Supporting Details
10.6	The Firm has a process to manage IT assets through removal, transfers, and disposition.	Shared	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. Reference: NIST SP 800-53 rev.3 FedRAMP Control: CM-1
10.7	The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities.	Shared	Network and service flaw remediation maintenance is controlled by deploying patches provided by Amazon Stewards for the appropriate security fixes. 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
10.8	The Firm's information security policy and training address removable and mobile media.	Shared	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 are 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

Question No.	Requirement	Responsibility	AWS Supporting Details
10.9	The Firm maintains controls to secure removable and portable media against malware and data leakage. If so, please briefly describe these controls.	Shared	AWS prevents unauthorized removal of maintenance equipment through the enforcement of the AWS Maintenance Policy, which prohibits maintenance equipment removal for offsite repairs. If maintenance equipment cannot be repaired onsite, the equipment is retired using the Media Sanitization and Destruction process. Reference: NIST SP 800-53 rev.3 FedRAMP Control: MA-3
10.10	The Firm maintains protection against Distributed Denial of Service (DDoS) attacks for critical internet-facing IP addresses. If so, please describe the internet functions protected and who provides this protection.	Shared	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
10.11	The Firm maintains a written data destruction policy.	Shared	Any digital media component leaving the controlled data center is sanitized and destroyed (e.g., degaussing, shredded, etc.) as defined in the AWS Media Protection policy. Reference: NIST SP 800-53 rev.3 FedRAMP Control: MA-04

Question No.	Requirement	Responsibility	AWS Supporting Details
10.12	The Firm maintains a written cybersecurity incident response policy. If so, please provide a copy of the policy and indicate the year in which it was most recently updated. Please also indicate whether the Firm conducts tests or exercises to assess its incident response policy, and if so, when and by whom the last such test or assessment was conducted.	Shared	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. Reference: NIST SP 800-53 rev.3 FedRAMP Control: IR-1
10.13	The Firm periodically tests the functionality of its backup system. If so, please provide the month and year in which the backup system was most recently tested.	Shared	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 customer 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)
11	Please indicate whether the Firm makes use of encryption. If so, what categories of data, communications, and devices are encrypted and under what circumstances?	Customer Specific	

Question No.	Requirement	Responsibility	AWS Supporting Details
12	Please indicate whether the Firm conducts periodic audits of compliance with its information security policies. If so, in what month and year was the most recent such audit completed, and by whom was it conducted?	Shared	The AWS cloud infrastructure has been designed and managed in alignment with regulations, standards, and best practices including: HIPAA, SOC, PCI, ISO, FedRAMP, etc. For more information see: http://aws.amazon.com/compliance/
Section 3	**Risks associated with remote customer access and funds transfer requests**		
Question No.	**Requirement**	**Responsibility**	**AWS Supporting Details**
13	Please indicate whether the Firm provides customers with on-line account access. If so, please provide the following information: a) The name of any third party or parties that manage the service. b) The functionality for customers on the platform (e.g., balance inquiries, address and contact information changes, beneficiary changes, transfers among the customer's accounts, withdrawals or other external transfers of funds). c) How customers are authenticated for on-line account access and transactions. d) Any software or other practice employed for detecting anomalous transaction requests that may be the result of compromised customer account access. e) A description of any security measures used to protect customer PINs stored on the sites. f) Any information given to customers about reducing cybersecurity risks in conducting transactions/business with the Firm.	Customer Specific	
14	Please provide a copy of the Firm's procedures for verifying the authenticity of email requests seeking to transfer customer funds. If no written procedures exist, please describe the process	Customer Specific	

Question No.	Requirement	Responsibility	AWS Supporting Details
15	Please provide a copy of any Firm policies for addressing responsibility for losses associated with attacks or intrusions impacting customers. 1. Does the Firm offer its customers a security guarantee to protect them against hacking of their accounts? If so, please provide a copy of the guarantee if one exists and a brief description.	Customer Specific	
Section 4	**Risks Associated With Vendors and Other Third Parties**		
Question No.	**Requirement**	**Responsibility**	**AWS Supporting Details**
16	If the Firm conducts or requires cybersecurity risk assessments of vendors and business partners with access to the Firm's networks, customer data, or other sensitive information, or due to the cybersecurity risk of the outsourced function, please describe who conducts this assessment, when it is required, and how it is conducted. If a questionnaire is used, please provide a copy. If assessments by independent entities are required, please describe any standards established for such assessments.	Shared	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
17	If the Firm regularly incorporates requirements relating to cybersecurity risk into its contracts with vendors and business partners, please describe these requirements and the circumstances in which they are incorporated. Please provide a sample copy.	Shared	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, security and business requirements specific to the procured technology. Reference: NIST SP 800-53 rev.3 FedRAMP Control: SA-4 (1)

Question No.	Requirement	Responsibility	AWS Supporting Details
18	Please provide a copy of policies and procedures and any training materials related to information security procedures and responsibilities for trainings conducted since January 2013 for vendors and business partners authorized to access its network.	Shared	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
19	If the Firm assesses the segregation of sensitive network resources from resources accessible to third parties, who (business group/title) performs this assessment, and provide a copy of any relevant policies and procedures?	Customer Specific	
20	If vendors, business partners, or other third parties may conduct remote maintenance of the Firm's networks and devices, describe any approval process, logging process, or controls to prevent unauthorized access, and provide a copy of any relevant policies and procedures.	Shared	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

Section 5	Detection of Unauthorized Activity		
For each of the following practices employed by the Firm to assist in detecting unauthorized activity on its networks and devices, please briefly explain how and by whom (title, department and job function) the practice is carried out.			
Question No.	**Requirement**	**Responsibility**	**AWS Supporting Details**
21.1	Identifying and assigning specific responsibilities, by job function, for detecting and reporting suspected unauthorized activity.	Shared	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. Reference: NIST SP 800-53 rev.3 FedRAMP Control: IR-1
21.2	Maintaining baseline information about expected events on the Firm's network.	Shared	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
21.3	Aggregating and correlating event data from multiple sources.	Shared	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

Question No.	Requirement	Responsibility	AWS Supporting Details
21.4	Establishing written incident alert thresholds.	Shared	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
21.5	Monitoring the Firm's network environment to detect potential cybersecurity events.	Customer Specific	
21.6	Monitoring the Firm's physical environment to detect potential cybersecurity events	Shared	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

Question No.	Requirement	Responsibility	AWS Supporting Details
21.7	Using software to detect malicious code on Firm networks and mobile devices	Shared	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
21.8	Monitoring the activity of third party service providers with access to the Firm's networks	Customer Specific	
21.9	Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm's networks.	Shared	AWS has implemented a variety of controls to ensure that unusual connections, connection attempts, access, and access attempts are monitored and reported. These include for DDoS attacks, web routing and traffic analysis, port scanning), host monitoring, performance monitoring, connection attempts and setting limits on allowed access attempts and setting alarming actions. Reference: NIST SP 800-53 rev.3 FedRAMP Control: CA-3
21.10	Evaluating remotely-initiated requests for transfers of customer assets to identify anomalous and potentially fraudulent requests.	Customer Specific	
21.11	Using data loss prevention software.	Customer Specific	

Question No.	Requirement	Responsibility	AWS Supporting Details
21.12	Conducting penetration tests and vulnerability scans. If so, please identify the month and year of the most recent penetration test and recent vulnerability scan, whether they were conducted by Firm employees or third parties, and describe any findings from the most recent risk test and/or assessment that were deemed to be potentially moderate or high risk but have not yet been addressed.	Shared	AWS scans host operating systems, web applications, and databases for vulnerabilities within the system boundary on a monthly basis. AWS Security Team conducts penetration testing on the infrastructure for further assurance that vulnerabilities not identified by the aforementioned scanning methods are identified. Reference: NIST SP 800-53 rev.3 FedRAMP Control: RA-5
21.13	Testing the reliability of event detection processes. If so, please identify the month and year of the most recent test.	Shared	AWS has implemented a variety of controls to ensure that unusual connections, connection attempts, access, and access attempts are monitored and reported. These include for DDoS attacks, web routing and traffic analysis, port scanning), host monitoring, performance monitoring, connection attempts and setting limits on allowed access attempts and setting alarming actions. Reference: NIST SP 800-53 rev.3 FedRAMP Control: CA-3
21.14	Using the analysis of events to improve the Firm's defensive measures and policies.	Shared	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. Reference: NIST SP 800-53 rev.3 FedRAMP Control: IR-04

Section 6	Other		
Question No.	**Requirement**	**Responsibility**	**AWS Supporting Details**
22	Did the Firm update its written supervisory procedures to reflect the Identity Theft Red Flags Rules, which became effective in 2013 (17 CFR § 248—Subpart C—Regulation S-ID)? 1. If not, why?	Customer Specific	
23	How does the Firm identify relevant best practices regarding cybersecurity for its business model?	Customer Specific	
24	Since January 1, 2013, has your Firm experienced any of the following types of events? If so, please provide a brief summary for each category listed below, identifying the number of such incidents (approximations are acceptable when precise numbers are not readily available) and describing their significance and any effects on the Firm, its customers, and its vendors or affiliates. If the response to any one item includes more than 10 incidents, the respondent may note the number of incidents and describe incidents that resulted in losses of more than $5,000, the unauthorized access to customer information, or the unavailability of a Firm service for more than 10 minutes. The record or description should, at a minimum, include: the extent to which losses were incurred, customer information accessed, and Firm services impacted; the date of the incident; the date the incident was discovered and the remediation for such incident.		
24.1	Malware was detected on one or more Firm devices. Please identify or describe the malware.	Customer Specific	
24.2	Access to a Firm web site or network resource was blocked or impaired by a denial of service attack. Please identify the service affected, and the nature and length of the impairment	Customer Specific	
24.3	The availability of a critical Firm web or network resource was impaired by a software or hardware malfunction. Please identify the service affected, the nature and length of the impairment, and the cause.	Customer Specific	
24.4	The Firm's network was breached by an unauthorized user. Please describe the nature, duration, and consequences of the breach, how the Firm learned of it, and how it was remediated.	Customer Specific	
24.5	The compromise of a customer's or vendor's computer used to remotely access the Firm's network resulted in fraudulent activity, such as efforts to fraudulently transfer funds from a customer account or the submission of fraudulent payment requests purportedly on behalf of a vendor.	Customer Specific	

Question No.	Requirement	Responsibility	AWS Supporting Details
24.6	The Firm received fraudulent emails, purportedly from customers, seeking to direct transfers of customer funds or securities.	Customer Specific	
24.7	The Firm was the subject of an extortion attempt by an individual or group threatening to impair access to or damage the Firm's data, devices, network, or web services	Customer Specific	
24.8	An employee or other authorized user of the Firm's network engaged in misconduct resulting in the misappropriation of funds, securities, sensitive customer or Firm information, or damage to the Firm's network or data.	Customer Specific	
25	Since January 1, 2013, if not otherwise reported above, did the Firm, either directly or as a result of an incident involving a vendor, experience the theft, loss, unauthorized exposure, or unauthorized use of or access to customer information? Please respond affirmatively even if such an incident resulted from an accident or negligence, rather than deliberate wrongdoing. If so, please provide a brief summary of each incident or a record describing each incident.		
26	For each event identified in response to Questions 24 and 25 above, please indicate whether it was reported to the following:		
26.1	Law enforcement (please identify the entity)	Customer Specific	
26.2	FinCEN (through the filing of a Suspicious Activity Report)	Customer Specific	
26.3	Financial Industry Regulatory Authority (FINRA)	Customer Specific	
26.4	A state or federal regulatory agency (please identity the agency and explain the manner of reporting)	Customer Specific	
26.5	An industry or public-private organization facilitating the exchange of information about cybersecurity incidents and risks	Customer Specific	

Appendix A: Additional AWS Services

- Amazon Relational Database Service (RDS): A service that makes it easy to set up, operate, and scale a relational database in the AWS cloud. It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks.

- Amazon DynamoDB: A fully-managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB enables customers to offload the administrative burdens of operating and scaling distributed databases to AWS, so they don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling.

- Amazon SimpleDB: A highly available and flexible non-relational data store that offloads the work of database administration. Developers simply store and query data items via web services requests and SimpleDB does the rest. Unbound by the strict requirements of a relational database, SimpleDB is optimized to provide high availability and flexibility, with little or no administrative burden.

- Elastic Load Balancing (ELB): ELB automatically distributes incoming application traffic across multiple EC2 instances. It enables AWS customers to achieve even greater fault tolerance in applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. ELB detects unhealthy instances within a pool and automatically reroutes traffic to healthy instances until the unhealthy instances have been restored. AWS customers can enable ELB within a single availability zone or across multiple zones for even more consistent application performance.

- Amazon Elastic MapReduce (EMR): A web service that enables businesses, researchers, data analysts, and developers to process vast amounts of data. It utilizes a hosted Hadoop framework running on the web-scale infrastructure of EC2 and S3.

- AWS Direct Connect: Direct Connect makes it easy to establish a dedicated network connection from customer premises to AWS. Using Direct Connect, customers can establish private connectivity between AWS infrastructure and an internal datacenter, office, or colocation environment.

- Amazon Glacier: A storage service that provides secure and durable storage for data archiving and backup. In order to keep costs low, Glacier is optimized for data that is infrequently accessed and for which retrieval times of several hours are suitable.

- AWS CloudHSM: A service that helps customers to meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud.

- Amazon RedShift: A fast, fully managed, petabyte-scale data warehouse service.
  Additional information about AWS products can be found here.

AWS Resources

1. AWS Compliance Center
   https://aws.amazon.com/compliance/
2. AWS Security Center:
   https://aws.amazon.com/security/
3. AWS Document Center
   https://aws.amazon.com/documentation/
4. Risk and Compliance Whitepaper:
   https://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf
5. Cloud Architecture Best Practices Whitepaper:
   https://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf
6. AWS Products Overview:
   https://aws.amazon.com/products/
7. AWS IAM Documentation:
   https://aws.amazon.com/documentation/iam/
8. AWS Sales and Business Development:
   https://aws.amazon.com/compliance/contact/public-sector/