Regulation Systems Compliance and Integrity Considerations for the AWS Cloud

November 2017

We welcome your feedback. Please share your thoughts at this link.

Notices

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

Contents

Abstract

This document provides information to assist SCI entities with running applications and services on the AWS cloud.

Introduction

The U.S. Securities and Exchange Commission adopted Regulation Systems Compliance and Integrity (Reg SCI) to strengthen the technology infrastructure of the U.S. securities markets. Reg SCI applies to entities that operate the core components of the securities markets, including national securities exchanges, clearing agencies, securities information processors, and alternative trading systems. These SCI entities are required to adopt an IT governance framework and system controls that ensure an adequate level of integrity, availability, resiliency, capacity, and security for systems that are necessary to maintain a fair and orderly securities market. SCI entities must monitor systems for disruptions, intrusions, and compliance events and report these instances to the SEC and impacted market participants. You should review the full text of Reg SCI here available here: https://www.sec.gov/rules/final/2014/34-73639.pdf. This document is not legal advice.

Security and Shared Responsibility

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

In order to help customers establish, operate and leverage the AWS security control environment, AWS has developed a security assurance program that uses global privacy and data protection best practices. These security protections and control processes are independently validated by multiple third-party independent assessments.

Customers can review and download reports and details about more than 2,500 security controls by using AWS Artifact, the automated compliance reporting tool available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS' security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, AWS MAS TRM Workbook, and certifications from accreditation bodies across geographies and compliance verticals.

Governance and Monitoring

While SCI entities are ultimately responsible for establishing a governance framework and monitoring their own environments, AWS provides many tools to help customers efficiently achieve compliance. For example, AWS Config helps customers continuously monitor and record their AWS resource configurations and automate the evaluation of recorded configurations against desired configurations. Amazon CloudWatch allows customers to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. Customers use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health.

AWS provides up-to-the-minute information on the AWS services that customers use to power their applications via the publicly available Service Health Dashboard. Customers can configure a Personal Health Dashboard to receive a personalized view of the performance and availability of the AWS services underlying their resources and applications. The dashboard displays relevant and timely information to help customers manage events in progress, and it provides proactive notification to help customers plan for scheduled activities. With Personal Health Dashboard, changes in the health of AWS resources automatically trigger alerts, providing event visibility and guidance to help quickly diagnose and resolve issues. Customers can use these insights to react and keep their applications running smoothly.

AWS Regions

The AWS Cloud infrastructure is built around Regions and Availability Zones (“AZs”). A Region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases which are more highly available, fault tolerant and scalable than would be possible from a single data center. The AWS Cloud operates 42 Availability Zones within 16 geographic Regions around the world.

For current information on AWS Regions and AZs, see https://aws.amazon.com/about-aws/global-infrastructure/.

Business Continuity and Disaster Recovery

SCI entities must implement policies and procedures to ensure that their applicable systems have high levels of resiliency and availability. Customers utilize AWS to enable faster disaster recovery of their IT systems without incurring the infrastructure expense of a second physical site. With data centers in regions all around the world, AWS provides a set of cloud-based disaster recovery services that enable rapid recovery of customers' IT infrastructure and data. The AWS cloud supports many popular disaster recovery architectures, from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover.

Conclusion

Proper Reg SCI implementation depends on the customer's ability to leverage the resilient, secure, and elastic solutions that AWS provides. Customers can decrease their operational risk and increase the security, availability and resiliency of their systems by running well-architected applications on the AWS Cloud.

Customers can optionally enroll in an Enterprise Agreement with AWS, which customers can use to tailor agreements that best suit their needs. For additional information on Enterprise Agreements please contact a sales representative.

.

Reg SCI Workbook

The Reg SCI Workbook provides additional information to help customers map their alignment to Reg SCI. This is not legal or compliance advice. Customers should consult with their legal and compliance teams.

Requirement Reference	Requirement	Implementation	Implementation Considerations
Obligations related to policies and procedures of SCI entities.			
§ 242.1001(a)(1)	Each SCI entity shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems and, for purposes of security standards, indirect SCI systems, have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets. Policies and procedures required by this section shall include, at a minimum:	Shared Responsibility	AWS has established an information security management program with designated roles and responsibilities that are appropriately aligned within the organization. AWS management reviews and evaluates the risks identified in the risk management program at least annually. Detailed information is provided in the AWS Security Whitepaper, https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf. Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In the case of failure, automated processes move customer data traffic away from the affected area. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are typically physically separated within a metropolitan region and are in different flood plains. Customers utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the

Requirement Reference	Requirement	Implementation	Implementation Considerations
			infrastructure expense of a second physical site. The AWS cloud supports many popular disaster recovery (DR) architectures, from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover. To learn more about AWS Disaster Recovery, see http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf.
§ 242.1001 (a)(2)(i)	The establishment of reasonable current and future technological infrastructure capacity planning estimates.	Shared Responsibility	AWS continuously monitors service usage to project infrastructure needs to support availability commitments and requirements. AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements. Customers are responsible for capacity planning for their application. In addition to on-demand capacity, AWS offers Reserved Instances (RI); RIs can provide a capacity reservation, offering additional confidence in your ability to launch the number of instances you have reserved when you need them.
§ 242.1001 (a)(2)(ii)	Periodic capacity stress tests of such systems to determine their ability to process transactions in an accurate, timely, and efficient manner.	Shared Responsibility	Customers should consider using Elastic Load Balancing (ELB). ELB automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables you to achieve fault tolerance in your applications, seamlessly providing the required amount of load balancing capacity needed to route application traffic.

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 242.1001 (a)(2)(iii)	A program to review and keep current systems development and testing methodology for such systems.	Shared Responsibility	AWS employs a shared responsibility model for data ownership and security. AWS operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS Services in production operations are managed in a manner that preserves their confidentiality, integrity and availability. AWS has implemented secure software development procedures that are followed to ensure appropriate security controls are incorporated into the application design. As part of the application design process, new applications must participate in an AWS Security review including registering the application, initiating the application risk classification, participating in the architecture review and threat modeling, performing code review, and performing a penetration test. Customers assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS-provided security group firewalls and other security, change management, and logging features.
§ 242.1001 (a)(2)(iv)	Regular reviews and testing, as applicable, of such systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters.	Shared Responsibility	AWS tests the Business Continuity plan and its associated procedures at least annually to ensure effectiveness of the plan and the organization readiness to execute the plan. Testing consists of engagement drills that execute on activities that would be performed in an actual outage. AWS documents the results, including lessons learned and any corrective actions that were completed. As previously stated, customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. Customers can request permission to conduct penetration testing to or

Requirement Reference	Requirement	Implementation	Implementation Considerations
			originating from any AWS resources as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Penetration tests should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans. Advance approval for these types of scans can be initiated by submitting a request using the AWS Vulnerability / Penetration Testing Request Form found here: https://aws.amazon.com/security/penetration-testing/.
§ 242.1001 (a)(2)(v)	Business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption;	Shared Responsibility	Learn how to architect DR in the AWS Cloud based on your specific requirements, https://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf Also consider the use of ELB health checks on their target EC2 instances, and detect whether or not an instance and the app running on it are healthy, combined with Auto Scaling groups to identify failing instances and cycle them out automatically, with limited downtime."
§ 242.1001 (a)(2)(vi)	Standards that result in such systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates the successful collection, processing, and dissemination of market data; and	Customer Responsibility	

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 242.1001 (a)(2)(vii)	Monitoring of such systems to identify potential SCI events.	Shared Responsibility	One way to monitor your systems includes the use of Amazon CloudWatch, a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly. Visit here to learn more: https://aws.amazon.com/cloudwatch/
§ 242.1001 (a)(3)	Each SCI entity shall periodically review the effectiveness of the policies and procedures required by this paragraph (a), and take prompt action to remedy deficiencies in such policies and procedures.	Customer Responsibility	

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 242.1001 (a)(4)	For purposes of this paragraph (a), such policies and procedures shall be deemed to be reasonably designed if they are consistent with current SCI industry standards, which shall be comprised of information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization. Compliance with such current SCI industry standards, however, shall not be the exclusive means to comply with the requirements of this paragraph (a).	Customer Responsibility	
§ 242.1001 (b)	Each SCI entity shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Act and the rules and regulations thereunder and the entity's rules and governing documents, as applicable.	Customer Responsibility	
§ 242.1001 (c)	Each SCI entity shall establish, maintain, and enforce reasonably designed written policies and procedures that include the criteria for identifying responsible SCI personnel, the designation and documentation of responsible SCI personnel, and escalation procedures to quickly inform responsible SCI personnel of potential SCI events.	Customer Responsibility	

Requirement Reference	Requirement	Implementation	Implementation Considerations
Obligations related to SCI event			
§ 242.1002 (a)	**Upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred**, each SCI entity shall begin to take appropriate corrective action which shall include, at a minimum, mitigating potential harm to investors and market integrity resulting from the SCI event and devoting adequate resources to remedy the SCI event as soon as reasonably practicable.	Shared Responsibility	The AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. The Service Health Dashboard is publicly available and displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources. The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan for scheduled activities. With Personal Health Dashboard, alerts are automatically triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues.
§ 242.1002(b)	Commission notification and recordkeeping of SCI events. Each SCI entity shall (1) notify the Commission of such SCI event immediately. (2) Within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that the SCI event has occurred, submit a written notification pertaining to such SCI event to the Commission, which shall be made on a good faith. (3) Until such time as the SCI event is resolved and the SCI entity's investigation of the SCI event is closed, provide updates pertaining to such SCI event to the Commission on a regular basis, or at such frequency as reasonably requested by a representative of the Commission. (4) Continue to communicate action with the Commission until a final report is issued. (5) Make, keep, and preserve records relating to all such SCI events.	Customer Responsibility	Amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as $0.004 per gigabyte per month, a significant savings compared to on-premises solutions. To keep costs low yet suitable for varying retrieval needs, Amazon Glacier provides three options for access to archives, from a few minutes to several hours. Learn more here https://aws.amazon.com/glacier/details/#Vault_Lock

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 242.1002 (c)	Promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event that is a systems disruption or systems compliance issue has occurred, disseminate follow the requirements setforth within for dissemination of SCI events.	Customer Responsibility	
Obligations related to systems changes; SCI review			
§ 242.1003 (a)	Within 30 calendar days after the end of each calendar quarter, each SCI entity submit to the Commission a report describing completed, ongoing, and planned material changes to its SCI systems and the security of indirect SCI systems, during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement and completion. An SCI entity shall establish reasonable written criteria for identifying a change to its SCI systems and the security of indirect SCI systems as material and report such changes in accordance with such criteria.	Customer Responsibility	Customers can use the AWS Service Health Dashboard for detailed information on service disruptions.
§ 242.1003 (b)	Each SCI entity shall: conduct an SCI review of the SCI entity's compliance with Regulation SCI not less than once each calendar year; provided, however, that: (i) Penetration test reviews of the network, firewalls, and production systems shall be conducted at a frequency of not less than once every three years; and (ii) Assessments of SCI systems directly supporting market regulation or market surveillance shall be conducted at a frequency based upon the risk assessment conducted as part of the SCI review, but in no case less than once every three years; and (2) Submit a report of the SCI review required by paragraph (b)(1) of this section to senior management of the SCI entity for review no more	Shared Responsibility	AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation

Requirement Reference	Requirement	Implementation	Implementation Considerations
	than 30 calendar days after completion of such SCI review; and (3) Submit to the Commission, and to the board of directors of the SCI entity or the equivalent of such board, a report of the SCI review required by paragraph (b)(1) of this section, together with any response by senior management, within 60 calendar days after its submission to senior management of the SCI entity.		can be performed by leveraging these reports and certifications. Included in these audit reports is Vulnerability Management. The AWS Security team notifies and coordinates with the appropriate Service Teams when conducting security-related activities within the system boundary. Activities include, vulnerability scanning, contingency testing, and incident response exercises. AWS performs external vulnerability assessments at least quarterly and identified issues are investigated and tracked to resolution. Additionally, AWS performs unannounced penetration tests by engaging independent third-parties to probe the defenses and device configuration settings within the system. AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at: http://aws.amazon.com/security/vulnerability-reporting/.
SCI entity business continuity and disaster recovery plans testing requirements for members or participants			
§ 242.1004	With respect to an SCI entity's business continuity and disaster recovery plans, including its backup systems, each SCI entity shall: (a) Establish standards for the designation of those members or participants that the SCI entity reasonably determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of such plans; (b) Designate members or participants pursuant to the standards established in paragraph (a) of this section and require participation by such designated members or participants in scheduled functional and performance testing of the operation of such	Customer Responsibility	

Requirement Reference	Requirement	Implementation	Implementation Considerations
	plans, in the manner and frequency specified by the SCI entity, provided that such frequency shall not be less than once every 12 months; and (c) Coordinate the testing of such plans on an industry- or sector-wide basis with other SCI entities.		
Recordkeeping requirements related to compliance with Regulation SCI			
§ 242.1005	(a) An SCI SRO shall make, keep, and preserve all documents relating to its compliance with Regulation SCI as prescribed in §240.17a-1 of this chapter.An SCI entity that is not an SCI SRO shall: (1) Make, keep, and preserve at least one copy of all documents, including correspondence, memoranda, papers, books, notices, accounts, and other such records, relating to its compliance with Regulation SCI, including, but not limited to, records relating to any changes to its SCI systems and indirect SCI systems; (2) Keep all such documents for a period of not less than five years, the first two years in a place that is readily accessible to the Commission or its representatives for inspection and examination; and	Customer Responsibility	Amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as $0.004 per gigabyte per month, a significant savings compared to on-premises solutions. To keep costs low yet suitable for varying retrieval needs, Amazon Glacier provides three options for access to archives, from a few minutes to several hours. Learn more here https://aws.amazon.com/glacier/details/#Vault_Lock
Electronic filing and submission			

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 242.1006	(a) Except with respect to notifications to the Commission made pursuant to § 242.1002(b)(1) or updates to the Commission made pursuant to paragraph § 242.1002(b)(3), any notification, review, description, analysis, or report to the Commission required to be submitted under Regulation SCI shall be filed electronically on Form SCI (§249.1900 of this chapter), include all information as prescribed in Form SCI and the instructions thereto, and contain an electronic signature; and (b) The signatory to an electronically filed Form SCI shall manually sign a signature page or document, in the manner prescribed by Form SCI, authenticating, acknowledging, or otherwise adopting his or her signature that appears in typed form within the electronic filing. Such document shall be executed before or at the time Form SCI is electronically filed and shall be retained by the SCI entity in accordance with § 242.1005.	Customer Responsibility	
Requirements for service bureaus			
§ 242.1007	If records required to be filed or kept by an SCI entity under Regulation SCI are prepared or maintained by a service bureau or other recordkeeping service on behalf of the SCI entity, the SCI entity shall ensure that the records are available for review by the Commission and its representatives by submitting a written undertaking, in a form acceptable to the Commission, by such service bureau or other recordkeeping service, signed by a duly authorized person at such service bureau or other recordkeeping service. Such a written undertaking shall include an agreement by the service bureau to permit the Commission and its representatives to examine such records at any time or from time	Customer Responsibility	

Requirement Reference	Requirement	Implementation	Implementation Considerations
	to time during business hours, and to promptly furnish to the Commission and its representatives true, correct, and current electronic files in a form acceptable to the Commission or its representatives or hard copies of any or all or any part of such records, upon request, periodically, or continuously and, in any case, within the same time periods as would apply to the SCI entity for such records. The preparation or maintenance of records by a service bureau or other recordkeeping service shall not relieve an SCI entity from its obligation to prepare, maintain, and provide the Commission and its representatives access to such records.		

Document Revisions

Date	Description
November 2017	First publication