Microsoft Azure

Regulation Systems Compliance and Integrity (SCI) Cloud Implementation Guide

Microsoft

Contents

Disclaimer

Contributors

The following Microsoft employees collaborated to create this document which provides guidance on meeting the Regulation Systems Compliance and Integrity (SCI) requirements in Microsoft Azure.

Written By:

Jeffrey Gallucci (Principal Program Manager, Azure Global, Microsoft)

Robert Arco (Senior Program Manager, Azure Global, Microsoft)

Reviewed By:

Derek Harris (Senior Attorney, CELA, Microsoft)

Introduction

Microsoft Azure is built with resiliency and availability as core principles which make our cloud services capable of meeting most any customer's needs across any industry in the world. We are continuously audited by independent third-party assessors across our myriad of services and against many global standards and regulatory requirements. To that end, Azure is tested and verified as a reliable and robust environment for our customers to build and innovate upon, to include putting their most key applications when speed, availability, and overall resiliency matter most. As will be described below, our Azure customers must make the choices to deploy in the manner that most suites their needs. However, Azure provides the options and opportunities for customers to bootstrap their enterprise key applications in such a way that they can confidently assure their regulators, their customers, and their leadership that key applications will function as designed and will be available when needed.

This document is meant to provide customers who must address and comply with the SEC's Regulation Systems Compliance and Integrity (SCI) with an overview of the Microsoft Azure features and services available to them to help enable their success and compliance. The U.S. SEC adopted Regulation SCI and Form SCI in November 2014 to strengthen the technology infrastructure of the U.S. securities markets. The Regulation SCI is designed to reduce the frequency of system incidents, improve resiliency when incidents do occur, and increase the SEC's oversight and enforcement of securities market technology infrastructure. For more detailed information on this regulation, please refer to the official Regulation SCI document.

Security and Shared Responsibility

As computing environments move from on premises datacenters to cloud datacenters, the responsibility of security also shifts. Security is a shared responsibility by both the cloud provider and the customer, and security controls are designed to ensure solutions are built and maintained in ways that ensure function and security successfully coexist. For every application and solution, how much of that responsibility falls on the customer depends on the applicable model in Azure. From IaaS to SaaS and PaaS, it is the customer's duty to understand to what degree they are accountable for implementing the required controls. Microsoft appreciates the thought that must go into this effort, and to that end have made available much guidance to assist customers in navigating what often amounts to a risk assessment effort. For more information on this dynamic between cloud service provider and customers, please review the shared responsibilities for cloud computing white paper.

Business Continuity and Disaster Recovery

Azure has established programs for security, resiliency, capacity planning and maintaining service integrity for all supplied services. These areas have designated roles, SOPs, tracking, and are reviewed and tested for gaps or risks on a regular basis (and are tested as part of normal operational conditions in response to "live events" necessitating immediate action). These programs are audited and certified by a variety of commercial, government and legal requirements. Microsoft recognizes the need for our customers to be able to read, review, and understand how it is we provide the controls necessary for our customers in this area, and in all security control domains and have invested in the production of this material and in an interface to make this material as easily consumable as possible. Customers can begin that research and vetting of information on Azure security, disaster recovery, availability, related certifications, and overall compliance offering by starting on Microsoft's Trust Center. To start deep diving into actual certification reports, whitepapers, and other detailed artifacts, customers can also go directly to the Service Trust Portal which stores and makes available the Microsoft Cloud's various certification reports.

Governance and Monitoring

Azure Governance is a group of concepts and service offerings that are designed to enable management of Azure resources at scale. These services offer the foundation to organize and structure your subscriptions in a logical way, create and deploy re-usable and Azure native packages of resources, to define, audit and remediate your resources, and more. The Cloud Adoption Framework governance model identifies key areas of importance during the journey. Each area relates to different types of risks a company must address as it adopts more cloud services. The governance journey focuses on not only business risks, but also policy, compliance, and processes to ensure the security of the cloud. To find out more about these concepts and services, and how to enable and use each, please visit the Azure Governance Documentation.

Azure Regions

An Azure region is a set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network. With more global regions than any other cloud provider, Azure gives customers the flexibility to deploy applications where they need to—offering the scale needed to bring applications closer to users around the world, preserving data residency, and offering comprehensive compliance and resiliency options for customers. To find more information about Azure Regions, visit our website.

Availability Zones within each Azure region protect your applications and data from datacenter failures. A minimum of three physically separate zones in all enabled regions help ensure resiliency. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. Zone-redundant services replicate your applications and data across Availability Zones to protect from single-points-of-failure. With Availability Zones, Azure offers an industry best 99.99% VM uptime SLA. The full Azure SLA explains the guaranteed availability of Azure as a whole. For more information on Azure regions and which regions currently support Availability Zones, see the Availability Zones Overview.

Conclusion

As security controls and regulations continue to develop, Microsoft is committed to helping our customers adjust and adapt to these new requirements. The guidance within this document aims to make clear which control areas and regulatory aspects are addressed in part by Azure. By offering this mapping, customers can better know when they are positioned to shift responsibility normally owned when a customer operates fully on premise, to Azure. These conclusions can be drawn by virtue of the promises made by Azure in SLAs, and through use of the capabilities Azure services provide which our customers can leverage to accomplish their goals. We also aim to call out when a Reg SCI requirement will remain the customer's responsibility to meet (where Azure services do not have a direct role). Lastly, this document also seeks to point customers to Azure documentation and services that may be used to enable an action or technical solution EVEN if the customer still must shoulder the responsibility as it pertains to a particular Reg SCI requirement, i.e., the ways Azure can *help* customers meet their responsibilities.

Several links within this guidance document lead customers to publicly available information and documentation about Azure services and features, which can provide the tools to build the right environment which will meet their needs. However, here are several links up front for customers to use if they wish to jump right into their resiliency learning journey. This information can serve as a starting point for customers as they draw up, or possibly vet existing plans for deploying applications and workloads requiring strong resiliency, low latency, and high availability:

- Business continuity and disaster recovery (BCDR): Azure Paired Regions
- Design Reliable Azure Applications
- Azure Storage redundancy
- What are Availability Zones in Azure?
- Zone-redundant storage (ZRS): Highly available Azure Storage applications
- Designing highly available applications using RA-GRS
- SLA for Virtual Machines

Reg SCI Reference	§ 242.1001 Obligations related to policies and procedures of SCI entities. (a) Capacity, integrity, resiliency, availability, and security.
Requirement Language	*(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.*
Ownership of Implementing	Shared Responsibility
Microsoft Azure Notes	Customers share the responsibility for addressing the controls for SCI via training, testing, and reporting, and through leveraging services and features available through Microsoft Azure, including those related to security, capacity, resiliency and availability. By doing so, customers can "maintain operational availability and promote the maintenance of fair and orderly markets". Azure services enable flexibility to place service instances and store data within multiple geographic paired regions as well as across multiple Availability Zones within each region. Availability Zones are designed as an independent failure zone providing localized transparent resiliency to common failures without necessitating geographic region failover. Customers can leverage a variety of Azure resiliency patterns and services to provide cost effective, risk-based recovery commensurate with the needs of their service criticality. This can include localized redundancy (Availability Zones), software load balancing, Virtual Machine Scale Sets (VMSS), Availability sets, active-active, active passive and a variety of schema's tailored to meet customer's availability needs (e.g., "Highly Available Cross-Premises and VNet-to-Vnet Connectivity". Azure also provides a variety of storage backup and recovery services (Azure Backup) that address real time data capture as well as point in time snapshot backups enabling data integrity. Customers leverage the data resiliency that best meets the needs of the service requirements.
Requirement Language	*(2) Policies and procedures required by paragraph (a)(1) of this section shall include, at a minimum:* *(i)The establishment of reasonable current and future technological infrastructure capacity planning estimates;* *(ii)Periodic capacity stress tests of such systems to determine their ability to process transactions in an accurate, timely, and efficient manner;* *(iii)A program to review and keep current systems development and testing methodology for such systems;* *(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;* *(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;*

	(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 *(vii)Monitoring of such systems to identify potential SCI events.*
Ownership of Implementing	Shared Responsibility
Microsoft Azure Notes	(i) (ii) (iii) (iv) (v) (vi) Microsoft has a comprehensive and mature Business Continuity Management (BCM) program for the inventorying, scoping, planning and testing of services available to our customers, as well as for the administration of our internal business processes. The BCM program is ISO 22301 certified and supports a variety of government and commercial certifications as well. The BCM program addresses all aspects of business continuity, including: • People • Process • Technology • Data • Hardware • Geographic risk • Service risk Our services (where applicable) are geographically recoverable, and services that customers leverage as service building blocks have documented how the "customer responsible" services can be deployed in multiple regions for DR resilience. Customer responsible services and the varied methods for design are all public facing and are tracked as part of the BCM program ensuring the highest level of resiliency. All "customer responsible" recovery instructions are documented in various locations (go here to research Azure resiliency capabilities for customers). Customers requiring a 2 hour or less recovery time objective (RTO) can leverage Azure services to meet their needs. (vii) Azure provides varied means of illuminating service impacts to customers including Azure Monitor. In addition, an overview and guidance on the shared responsibility related to Incident Management between Microsoft and customers can be read about here.
Requirement Language	*(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.*
Ownership of Implementing	Shared Responsibility
Microsoft Azure Notes	Customer Driven
Requirement Language	*(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).
Ownership of Implementing	Shared Responsibility
Microsoft Azure Notes	While the customer, or "SCI Entity", holds the responsibility for implementing the controls described in this section of the regulation, Microsoft Azure's commitment to regulatory compliance can be researched on the Trust Center. Details on the assessment reports earned by Microsoft based off of many globally recognized standards and requirements, can be reviewed by accessing them via Service Trust Portal (STP) (only available to customers). The depth and breadth of Microsoft's compliance offerings underscore our deep understanding of worldwide regulatory complexities and needs.
Reg SCI Reference	§ 242.1001 Obligations related to policies and procedures of SCI entities. (b) Systems compliance.
Requirement Language	*(1) 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.*
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer Driven
Requirement Language	*(2) Policies and procedures required by paragraph (b)(1) of this section shall include, at a minimum:* *(i) Testing of all SCI systems and any changes to SCI systems prior to implementation;* *(ii) A system of internal controls over changes to SCI systems;* *(iii) A plan for assessments of the functionality of SCI systems designed to detect systems compliance issues, including by responsible SCI personnel and by personnel familiar with applicable provisions of the Act and the rules and regulations thereunder and the SCI entity's rules and governing documents; and* *(iv) A plan of coordination and communication between regulatory and other personnel of the SCI entity, including by responsible SCI personnel, regarding SCI systems design, changes, testing, and controls designed to detect and prevent systems compliance issues.*
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer can leverage Azure Services to test their systems deployed on Azure. For more information on how customers can test their resiliency capabilities, go here.
Requirement Language	*(3) Each SCI entity shall periodically review the effectiveness of the policies and procedures required by this paragraph (b), and take prompt action to remedy deficiencies in such policies and procedures.*
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer Driven

Requirement Language	*(4) Safe harbor from liability for individuals. Personnel of an SCI entity shall be deemed not to have aided, abetted, counseled, commanded, caused, induced, or procured the violation by an SCI entity of this paragraph (b) if the person: (i)Has reasonably discharged the duties and obligations incumbent upon such person by the SCI entity's policies and procedures; and (ii)Was without reasonable cause to believe that the policies and procedures relating to an SCI system for which such person was responsible, or had supervisory responsibility, were not established, maintained, or enforced in accordance with this paragraph (b) in any material respect. (c) Responsible SCI personnel. (1) 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. (2) Each SCI entity shall periodically review the effectiveness of the policies and procedures required by paragraph (c)(1) of this section, and take prompt action to remedy deficiencies in such policies and procedures.*
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer Driven
Reg SCI Reference	§ 242.1002 Obligations related to SCI entities. (a) Corrective action.
Requirement Language	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.
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	It is the customer and the SCI personnel's responsibility to take appropriate actions for any detected SCI event. Microsoft Azure Services can provide functionality to customers which can enable detection and monitoring of applicable events in a customer's environment. The following are some which may enable the customer in this space: - Azure Sentinel - Azure Monitor - Azure Security Center - Azure Service Health - Azure Network Watcher
Reg SCI Reference	§ 242.1002 Obligations related to SCI entities. (b) Commission notification and recordkeeping of SCI events.
Requirement Language	**Each SCI entity shall:**

	(1) Upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, 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, best efforts basis and include: (i) A description of the SCI event, including the system(s) affected; and (ii) To the extent available as of the time of the notification: the SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; the potential impact of the SCI event on the market; a description of the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved or timeframe within which the SCI event is expected to be resolved; and any other pertinent information known by the SCI entity about the SCI event; (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, to correct any materially incorrect information previously provided, or when new material information is discovered, including but not limited to, any of the information listed in paragraph (b)(2)(ii) of this section; (4) (i)(A) If an SCI event is resolved and the SCI entity's investigation of the SCI event is closed within 30 calendar days of the occurrence of the SCI event, then within five business days after the resolution of the SCI event and closure of the investigation regarding the SCI event, submit a final written notification pertaining to such SCI event to the Commission containing the information required in paragraph (b)(4)(ii) of this section. (B)(1) If an SCI event is not resolved or the SCI entity's investigation of the SCI event is not closed within 30 calendar days of the occurrence of the SCI event, then submit an interim written notification pertaining to such SCI event to the Commission within 30 calendar days after the occurrence of the SCI event containing the information required in paragraph (b)(4)(ii) of this section, to the extent known at the time. (2) Within five business days after the resolution of such SCI event and closure of the investigation regarding such SCI event, submit a final written notification pertaining to such SCI event to the Commission containing the information required in paragraph (b)(4)(ii) of this section. (ii) Written notifications required by paragraph (b)(4)(i) of this section shall include: (A) A detailed description of: the SCI entity's assessment of the types and number of market participants affected by the SCI event; the SCI entity's assessment of the impact of the SCI event on the market; the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event (5) i)(A) If an SCI event is resolved and the SCI entity's investigation of the SCI event is closed within 30 calendar days of the occurrence of the SCI event, then within five business days after the resolution of the SCI event and closure of the investigation regarding the SCI event, submit a final written notification pertaining to such SCI event to the Commission containing the information required in paragraph (b)(4)(ii) of this section. (B)(1) If an SCI event is not resolved or the SCI entity's investigation of the SCI event is not closed within 30 calendar days of the occurrence of the SCI event, then submit an interim written notification pertaining to such SCI event to the Commission within 30 calendar days after the occurrence of the SCI event containing the information required in paragraph (b)(4)(ii) of this section, to the extent known at the time. (2) Within five business days after the resolution of such SCI event and closure of the

	investigation regarding such SCI event, submit a final written notification pertaining to such SCI event to the Commission containing the information required in paragraph (b)(4)(ii) of this section. (ii) Written notifications required by paragraph (b)(4)(i) of this section shall include: (A) A detailed description of: the SCI entity's assessment of the types and number of market participants affected by the SCI event; the SCI entity's assessment of the impact of the SCI event on the market; the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	It is the customer and the SCI system personnel's responsibility to take appropriate actions for any detected SCI events impacting their environment, to include notification of the event and the ongoing status of the event to "the Commission". Microsoft will contribute in the requirement to detect, notify, and report on the event to the extent we are able, to include by providing our customers telemetry or other data related to Azure service uptime, outages, availability, or any other attainable and relevant data if appropriate. When an incident occurs that impacts our customers, actions are taken rapidly to ensure our customers have access to Microsoft personnel to address questions and incident status. Customers also have the ability to leverage Azure Service Health via Azure Portal. Azure Service Health can be configured by customers to provide alerts automatically notifying about service issues in various mediums (e.g., email, SMS, push notifications, etc.) in order to assist customer with Reg SCI requirements in fulfilling their needs. For specific and tailored needs related to events and notifications, Azure customers should contact their account representative to discuss options. To assist customers in detecting and monitoring events in their environment, the following are some of the Azure services which customers can leverage (not an exhaustive list): - Azure Sentinel - Azure Monitor - Azure Security Center - Azure Network Watcher
Reg SCI Reference	§ 242.1002 Obligations related to SCI entities. (c) Dissemination of SCI events.
Requirement Language	*(1) Each SCI entity shall: (i) 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 the following information about such SCI event: (A) The system(s) affected by the SCI event; and (B) A summary description of the SCI event; and (ii) When known, promptly further disseminate the following information about such SCI event: (A) A detailed description of the SCI event; (B) The SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; and (C) A description of the progress of its corrective action for the SCI event and when the SCI event has been or is expected to be resolved; and (iii)*

	Until resolved, provide regular updates of any information required to be disseminated under paragraphs (c)(1)(i) and (ii) of this section.
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer Driven Only
Requirement Language	*(2) Each SCI entity shall: (i) 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 the following information about such SCI event: (A) The system(s) affected by the SCI event; and (B) A summary description of the SCI event; and (ii) When known, promptly further disseminate the following information about such SCI event: (A) A detailed description of the SCI event; (B) The SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; and (C) A description of the progress of its corrective action for the SCI event and when the SCI event has been or is expected to be resolved; and (iii) Until resolved, provide regular updates of any information required to be disseminated under paragraphs (c)(1)(i) and (ii) of this section.*
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer Driven Only
Requirement Language	*(3)* The information required to be disseminated under paragraphs (c)(1) and (2) of this section promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event has occurred, shall be promptly disseminated by the SCI entity to those members or participants of the SCI entity that any responsible SCI personnel has reasonably estimated may have been affected by the SCI event, and promptly disseminated to any additional members or participants that any responsible SCI personnel subsequently reasonably estimates may have been affected by the SCI event; provided, however, that for major SCI events, the information required to be disseminated under paragraphs (c)(1) and (2) of this section shall be promptly disseminated by the SCI entity to all of its members or participants.
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer Driven Only
Requirement Language	*(4)* The requirements of paragraphs (c)(1) through (3) of this section shall not apply to: (i) SCI events to the extent they relate to market regulation or market surveillance systems; or (ii) Any SCI event that has had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants.
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer Driven Only
Reg SCI Reference	§ 242.1003 Obligations related to systems changes; SCI review.

	(a) Systems changes.
Requirement Language	*(1)* Within 30 calendar days after the end of each calendar quarter, 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. *(2)* Promptly submit a supplemental report notifying the Commission of a material error in or material omission from a report previously submitted under this paragraph (a).
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer Driven Only
Reg SCI Reference	§ 242.1003 Obligations related to systems changes; SCI review. (a) SCI review.
Requirement Language	Each SCI entity shall: (1) 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 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.
Ownership of Implementing	Shared Responsibility
Microsoft Azure Notes	Azure has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the Azure control environment. Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of Azure 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 Azure. The Azure audit reports identify the scope of Azure services and regions assessed, as well as the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications. Included in these audit reports is Vulnerability Management. The Azure 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. Azure performs external vulnerability assessments three times per year and

	identified issues are investigated and tracked to resolution. Additionally, Azure regularly performs unannounced penetration testing, known as Red Teaming, which is live site penetration test against Microsoft managed cloud infrastructure, services and applications. Azure Security teams also subscribe to newsfeeds for applicable vendors, and proactively monitor vendors' websites and other relevant outlets for new patches. Azure customers also have access to customer support in line with their support plan.
Reg SCI Reference	§ 242.1004 SCI Entity business continuity and disaster recovery plans testing requirements for members or participants. With respect to an SCI entity's business continuity and disaster recovery plans, including its backup systems, each SCI entity shall:
Requirement Language	(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 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.
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer Driven
Reg SCI Reference	§ 242.1005 Recordkeeping requirements related to compliance with Regulation SCI.
Requirement Language	(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. (b) 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 (3) Upon request of any representative of the Commission, promptly furnish to the possession of such representative copies of any documents required to be kept and preserved by it pursuant to paragraphs (b)(1) and (2) of this section. (c) Upon or immediately prior to ceasing to do business or ceasing to be registered under the Securities Exchange Act of 1934, an SCI entity shall take all necessary action to ensure that the records required to be made, kept, and preserved by this section shall be accessible to the Commission and its representatives in the manner required by this section and for the remainder of the period required by this section.
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	It is the customer and the SCI personnel's responsibility to put monitoring and archiving solutions in place. Microsoft Azure Services can provide functionality to customers which can enable detection, monitoring, and storage of applicable events in a customer's

	environment. Azure Archive Storage is a highly available secure cloud storage for scarcely accessed data that can assist with your varying retrieval needs.
Reg SCI Reference	§ 242.1006 Electronic filing and submission.
Requirement Language	(a) 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 (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)); 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.
Ownership of Implementing	Customer Responsibility
Microsoft Azure Notes	Customer Driven
Reg SCI Reference	§ 242.1007 Requirements for service bureaus.
Requirement Language	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 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.
Ownership of Implementing	Customer responsibility
Microsoft Azure Notes	Customer Driven

Glossary of Terms and Links

Link	Availability Sets	https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets#availability-set-overview
Link	Availability Zones Overview	https://azure.microsoft.com/en-us/global-infrastructure/availability-zones/
Link	Azure Archive Storage	https://azure.microsoft.com/en-us/services/storage/archive/
Link	Azure Backup	https://azure.microsoft.com/en-us/services/backup/
Link	Azure Governance Documentation	https://docs.microsoft.com/en-us/azure/governance/
Link	Azure Monitor	https://azure.microsoft.com/en-us/services/monitor/
Link	Azure Network Watcher	https://azure.microsoft.com/en-us/services/network-watcher/
Link	Azure Regions	https://azure.microsoft.com/en-us/global-infrastructure/regions/
Link	Azure Security Center	https://azure.microsoft.com/en-us/services/security-center/
Link	Azure Sentinel	https://azure.microsoft.com/en-us/services/azure-sentinel/
Link	Azure Service Health	https://azure.microsoft.com/en-us/features/service-health/
Link	Azure SLA	https://azure.microsoft.com/support/legal/sla/virtual-machines/
Link	Azure Storage redundancy	https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy
Link	Business Continuity and Disaster Recovery (BCDR): Azure Paired Regions	https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions
Link	Cloud Adoption Framework Governance Model	https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/journeys/index
Link	Design Reliable Azure Applications	https://docs.microsoft.com/en-us/azure/architecture/reliability/
Link	Designing Highly Available Applications Using RA-GRS	https://docs.microsoft.com/en-us/azure/storage/common/storage-designing-ha-apps-with-ragrs
Link	Highly Available Cross-Premises and VNet-to-Vnet Connectivity	https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable
Link	Incident Management	http://aka.ms/SecurityResponsepaper
Link	Load Balancing	https://azure.microsoft.com/en-us/services/load-balancer/
Link	Microsoft's Trust Center	https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings
Link	Regulation SCI	https://www.sec.gov/rules/final/2014/34-73639.pdf
Link	Resiliency Capabilities for Customers: Overview	https://docs.microsoft.com/en-us/azure/architecture/resiliency/
Link	Resiliency Capabilities for Customers: Test Capabilities	https://docs.microsoft.com/en-us/azure/architecture/resiliency/#test-for-resiliency
Link	Service Trust Portal	https://servicetrust.microsoft.com/
Link	Shared Responsibilities for Cloud Computing	https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91/file/153019/1/Shared responsibilities for cloud computing.pdf
Link	SLA for Virtual Machines	https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_8/
Link	Virtual Machine Scale Sets (VMSS)	https://azure.microsoft.com/en-us/services/virtual-machine-scale-sets/
Link	Zone-redundant storage (ZRS)	https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs