Amazon Web Services® (AWS®) Audit Program

Column Name	Description	Instructions
Process Sub-area	An activity within an overall process influenced by the enterprise's policies and procedures that takes inputs from a number of sources, manipulates the inputs and produces outputs	To make the audit program manageable, it is recommended to break out the scope of the audit into sub-areas. The auditor can modify this field to include enterprise-specific names and terms. ISACA has used the most commonly used terms as the basis to develop this audit program.
Ref. Risk	Specifies the risk this control is intended to address	This field can be used to input a reference/link to risk described in the enterprise's risk register or enterprise risk management (ERM) system, or to input a description of the risk that a particular control is intended to address.
Control Objectives	A statement of the desired result or outcome that must be in place to address the inherent risk in the review areas within scope	This field should describe the behaviors, technologies, documents or processes expected to be in place to address the inherent risk that is part of the audit scope. An IS audit manager can review this information to determine whether the review will meet the audit objectives based on the risk and control objectives included in the audit program.
Controls	The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management or legal nature	This field should describe in detail the control activities expected to be in place to meet the control objective. Control activities can be reflected in roles and responsibilities, documentation, forms, reports, system configuration, segregation of duties, approval matrices, etc. An IS audit manager performing a quality control review must decide whether an auditor has planned to identify a sufficient number of controls on which to base an assessment and whether the planned evidence is sufficiently objective.
Control Type	Controls can be automated (technical), manual (administrative) or physical. • Automated/technical controls are managed or performed by computer systems. • Manual/administrative controls usually reflect processes or actions that employees can or cannot take. • Physical controls include locks, fences, mantraps and even geographic-specific controls.	Specify whether the control under review is automated, manual or physical. This information is useful in determining the testing steps necessary to obtain assessment evidence.
Control Classification	Another way to classify controls is by the way they address a risk exposure. • Preventive controls should stop an event from happening. • Detective controls should identify an event after it has happened and generate an alert that triggers a corrective control. • Corrective controls should limit the impact of an event and help restore normal operations within a reasonable time frame. • Compensating controls are alternate controls designed to accomplish the intent of the original controls (as closely as possible) when the originally designed controls cannot be used due to limitations of the environment.	Specify whether the control under review is preventive, detective, corrective or compensating. This information will be helpful when defining testing steps and requesting evidence.
Control Frequency	Control activities can occur in real time, daily, weekly, monthly, annually, etc.	Specify whether the control under review occurs in real time, daily, weekly, monthly, annually, etc. This information will be helpful when defining testing steps and requesting evidence.

Amazon Web Services® (AWS®) Audit Program		
Column Name	***Description***	***Instructions***
Testing Step	Identifies the steps being tested to evaluate the effectiveness of the control under review	This field should describe in detail the steps necessary to test control activities and collect supporting documentation. The auditor can modify this field to meet enterprise-specific needs. ISACA has used a set of generic steps to develop this audit program. An IS audit manager may determine whether the proposed steps are adequate to review a particular control.
Ref. Framework/Standards	Specifies frameworks and/or standards that relate to the control under review (e.g., NIST, HIPAA, SOX, ISO)	Reference other frameworks used by the enterprise as part of its compliance program.
Ref. Workpaper	This field usually references documents that contain evidence supporting the pass/fail mark for the audit step.	Specify the location of supporting documentation detailing the audit steps and evidence obtained. An IS audit manager performing a quality control review must decide whether an auditor has tested a sufficient number of controls on which to base an assessment and whether the obtained evidence is sufficiently objective to support a pass or fail conclusion.
Pass/Fail	Document preliminary conclusions regarding the effectiveness of controls.	Specify whether the overall control is effective (pass) or not effective (fail), based on the results of the testing.
Comments	Free format field	Document any notes related to the review of this process sub-area or specific control activities.

Amazon Web Services® (AWS®) Audit Program
Disaster Recovery

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/ Fail	Comments
Disaster Recovery Plans: Stakeholder Input & Review		The enterprise mitigates the risk of being unable to resume operations when disaster occurs.	The enterprise has an AWS disaster recovery (DR) plan which it reviews on a periodic basis for completeness and accuracy. On a periodic basis, enterprise management participates in disaster recovery exercises and provides feedback to the business continuity department. Note: DR is IT-operations focused, in distinction to business continuity, which is business-operations focused. Each may negatively affect the other, but the impact of disaster recovery on business operations is typically more severe. DR plans should be developed that take a complete and accurate account of the potential impact resulting from disaster, as well as the needs of business operations affected by a disaster, as they recover. Actions documented and executed from the DR plan should seek to assist the business and its individual units in becoming acceptably functional in the least amount of time, at minimal cost.				1. Interview responsible and/or accountable individuals (business continuity, operational management, etc.) to determine level of required or actual participation of individual business units (sales, finance, AR, etc.), in the development and maintenance of the enterprise's disaster recovery activities. 2. Obtain and inspect disaster recovery plans, meeting minutes and/or recovery exercise summary reports to determine whether enterprise stakeholders are assisting the enterprise in creating effective disaster recovery plans. Evidence of stakeholder involvement may include: • Timestamped signoffs on disaster recovery plans, procedures or related documentation • Documented meeting minutes and calendar invites • Documented input from stakeholders that are later transcribed by the business continuity department into DR exercise reports				
Business Continuity Plans (BCPs)		Business operations can continue in the event of significant business disruption or can recover from a disaster.	The enterprise documents business continuity procedures and processes for individual business units to execute during disaster recovery. Note: Business units may have special procedures that need to be executed during or following IT-service restoration. Departmental knowledge of particular business systems or operations may facilitate order of execution by certain business units in a concerted or staggered fashion. These instances or circumstances should be detailed in individual procedures that are reviewed, refined and practiced during or near the time of disaster recovery exercises. [Robin: original statement in red above seemed garbled. Not sure I understood intent correctly.]				1, Interview responsible and/or accountable individuals (business continuity, operational management, etc.) to determine the: • Business-operational dependencies that may exist before or during certain stages of disaster recovery exercises • Potential unplanned events that the enterprise attempts to prepare for • Affected business processes that the enterprise may need to address through documented recovery instructions 2. Inquire of personnel responsible for developing and maintaining individual business continuity plans regarding the frequency of: • Reviews of business continuity plans • Business continuity/disaster recovery exercises 3. Obtain documentation of the population of business continuity plans by business unit or department with special attention to any missing business units or departments. Using a judgmental selection of business plans from this population, review the sample for: • Complete and accurate description of business critical processes requiring validation during or after a disaster • Detailed minimum level of recovery for individual processes or larger combined processes (for example, email capability required but fax capability not being required) • Detailed business process workarounds if primary methods remain unavailable • Documented practice exercises				
High Availability		The enterprise mitigates the risk of disruption to operations when disaster occurs.	The enterprise deploys critical AWS applications to multiple data centers physically secured by AWS. Note: AWS provides its services across multiple regions (large geographical areas such as Oregon) and availability zones (AWS-controlled data centers within the region). Enterprises can choose to deploy certain assets (such as an S3 bucket) to specific regions and availability zones for DR and availability purposes. For example, AWS Config and EC2 instances may be operational and deployed to the Northern Virginia region and certain data centers, but not in the Oregon region as required by the enterprise. This test seeks to determine whether critical assets are where they should be, and can remain available during a disaster.				1. Interview responsible and/or accountable individuals (architecture, networking, business continuity, etc.) to determine how the enterprise ensures or mitigates availability issues for its critical AWS applications during a disaster. Ensure that: • AWS applications and data are not stored in regions (Canada, EU, Asia-Pacific, US, etc.) which may introduce regulatory concerns • AWS applications and data are not deployed to availability zones lacking required security or configuration functionality • Methods are used to detect and correct events related to the conditions above (or other undesirable states defined by the enterprise) 2. Obtain documentation of the population of critical AWS applications. Through judgmental selection from this population, determine whether critical assets are completely and accurately fault tolerant and/or provide high availability through deployment to agreed-upon alternate locations (regions and availability zones, or other data centers) From the AWS Management Console: a. Select the AWS application or resource of interest. b. In the AWS Navigation Bar, scroll to the far right of the screen and click the down arrow next to the Region "N. Virginia", etc. 3. Determine if resources are deployed appropriately through inspection of individual resources in multiple regions.				
Alternating Responsible Personnel		Disaster recovery responsibilities are shared and rotated routinely to maximize availability potential of the enterprise's AWS applications.	Disaster recovery coordinators and core staff are cross-trained on their responsibilities and rotated on a periodic basis. Note: To ensure that appropriate knowledge and expertise are available when disaster strikes, multiple personnel should possess similar knowledge (possibly across multiple or very specific areas) sufficient to recover the enterprise's AWS applications and business processes. This may include two individuals with the same responsibilities or groups of three or more. These personnel should alternate between recovery exercises to ensure they adequately understand and can execute their responsibilities when needed.				1. Interview responsible and/or accountable individuals (business continuity, operational management, etc.) to determine the personnel, business units or departments that require alternate knowledge of business recovery processes and requirements. 2. Obtain and inspect completed training and/or evidence showing responsible individuals executed assigned recovery responsibilities as dictated by the enterprise.				

Amazon Web Services® (AWS®) Audit Program Disaster Recovery											
Process Sub-area	***Ref. Risk***	***Control Objectives***	***Controls***	***Control Type***	***Control Classification***	***Control Frequency***	***Testing Step***	***Ref. Framework/ Standards***	***Ref. Workpaper***	***Pass/ Fail***	***Comments***
Validating Backups		The enterprise's strategic objectives around data availability and integrity are met through formal data-protection and restoration planning.	The enterprise ensures critical data integrity through routinely scheduled test restorations of critical data (as part of the enterprise's periodic disaster recovery exercises). Note: The tests may center on critical data, generated in AWS applications, that are stored in third-party applications, vendor data centers or inside the enterprise's data center. Risk associated with backup-restoration failure can be tremendous and may require additional resources to deploy backup solutions such as Netapp.				1. Interview responsible and/or accountable individuals (business continuity, security, infrastructure, etc.) to determine if routine restoration of data backups occurs as part of disaster recovery efforts, to ensure backups will restore necessary data, if needed. 2. Inquire about in-scope systems or data and how completeness and accuracy of backup restoration is measured and documented. 3. Obtain and inspect disaster recovery exercise reports to determine if in scope systems and data were restored as required. 4. Obtain and inspect backup solution reports indicating successful restoration for in-scope systems and data.				
Managing Vendor Lock-in Risk		The enterprise ensures continuity of operations by contracting with additional cloud providers.	AWS applications and APIs are developed to be cross-compatible on multiple cloud platforms. Note: Cloud providers may engage in unacceptable practices or go out of business for various reasons (financial, breach, noncompetitive, etc.), leaving the enterprise with insufficient time to transfer or rebuild operations on another platform. Agile enterprises must ensure that they build and deploy cloud applications to transfer easily to another provider, if necessary.				1. Interview responsible and/or accountable individuals (business continuity, application development, infrastructure, etc.) to determine whether the AWS applications and related resources that the enterprise develops are completely and directly transferable to another cloud or noncloud provider (e.g., Azure®, Oracle®, Citrix®, etc.), and whether the enterprise spends time and effort ensuring that the alternate provider's platform provides a seamless business operational experience for enterprise users (internal or external). 2. Inquire about: • The minimum level of business-application functionality that must be operational and available in order for the enterprise to continue providing its services, and which AWS applications and related resources (APIs, data in AWS applications, etc.) those business functions relate to • The degree of business functionality that exists and is operational on the alternate provider's platform 3. Obtain and inspect disaster recovery reports indicating that failover tests, migrations or other functionality tests are routinely performed by the enterprise for critical AWS applications and related resources. 4. Obtain and inspect vendor contracts demonstrating that the enterprise has contracted with an alternate cloud provider for a similar service offering (i.e., similar types and volume of services are expected). 5. Observe critical business processes being completely and accurately executed on the alternate provider's platform. Alternatively, using a judgmental sample of business processes, request that the enterprise provide proof that business processes included in sample can be successfully executed on the alternate provider's platform.				

Amazon Web Services® (AWS®) Audit Program
Security Logging and Monitoring

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/ Fail	Comments
Defining Monitoring Requirements by AWS Application		Through its formal security monitoring program, the enterprise mitigates the risk that access to its data and systems is denied due to malicious acts.	The enterprise completely and accurately defines minimum monitoring requirements for AWS applications and related resources. AWS Monitoring requirements are formally documented and reviewed on a frequency predetermined by the enterprise. Note: Monitoring may include certain types of events, processes or API calls, or extend to higher-level attributes, such as source of event, account-making changes, date/time, etc.				1. Interview responsible and/or accountable individuals (security, operations management, etc.) to determine whether AWS applications in use and related resources have a minimum set of monitoring and logging requirements. Confirm that the monitoring and logging requirements are both formally documented and reassessed routinely for completeness and accuracy. 2. Inquire about: • In-scope AWS applications and related resources • Individuals responsible and methods used to identify new applications on which monitoring should be enabled • Any standards or frameworks used by the enterprise to derive monitoring baselines • Frequency of review against established monitoring requirements 2. Obtain documentation of the population of in-scope AWS applications and related resources. Through judgmental sampling, obtain and inspect enterprise documentation that details monitoring requirements for each in-scope AWS application and related resources.				
Configured Logging Requirements			The enterprise programmatically enforces minimum monitoring requirements through application configuration. AWS applications are configured to generate and retain monitored events required by the enterprise.				1. Interview responsible and/or accountable individuals (security, operations management, etc.) to determine how the enterprise's monitoring standards are enforced on an application-by-application basis. 2. Determine: • How the enterprise detects lack of compliance with monitoring standards • Timeliness of remediation upon discovery of noncompliance 3. Using the defined requirements gathered in the previous step, select a judgmental sample of AWS applications and determine whether the documented monitoring standards are enforced in each application.				
Log Storage		The enterprise ensures that its log-retention practices meet compliance requirements as well as business needs.	The enterprise retains logs generated by AWS applications in a secure, centralized location, using AWS Simple Storage Service (S3) buckets and AWS Glacier.				1. Interview responsible and/or accountable individuals to determine how log aggregation, retention and access security are managed, giving specific attention to the application destinations for generated monitoring logs. 2. Inquire whether: • Classification is performed on logs stored in each log-storage solution • Data-retention policies are enforced by classification in each log-storage solution • Short-term logging requirements (S3) and long-term storage requirements (Glacier) are identified and configured • Access is routinely reviewed for appropriateness for each log-storage solution 3. Using previously obtained documentation, obtain and inspect individual AWS application configurations to determine whether in-scope applications are configured to send logs to the appropriate log-storage solution. 4. Inspect data-retention settings to determine whether complete and accurate data transfer between short- to long-term storage is performed.				
Restricting Log Access		The enterprise maintains log integrity by limiting access to individuals with a valid business need.	Access to AWS logs is based on job responsibilities and least privilege, and is reviewed by management on a periodic basis.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine how access to logs generated by AWS applications and related resources is controlled, and identify the users or departments that should have access, based on job responsibilities. 2. Inquire about reviews of access for appropriateness and methods used to identify and remove inappropriate access. 3. Obtain and inspect access lists and inquire with management to determine appropriateness of access. 4. Obtain and inspect completed access reviews to determine that inappropriate access (once identified) is removed in a timely manner.				
Monitoring Log Status		The enterprise maintains log integrity through monitoring and investigating attempts to modify log data.	CloudWatch alarms are configured to notify appropriate groups or individual(s) when successful or failed attempts to alter log data occur. Note: Malicious users may attempt to cover their tracks during or after an attack by altering the bucket policy, deleting logs, overwriting logs, modifying alarm recipients, or changing alarm status (on/off) or other log settings.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine whether the enterprise has mechanisms in place that notify personnel and trigger timely investigations if alarms are triggered by attempts to modify logs or related security settings. 2. Inquire whether multifactor authentication DELETE requirements are in place for in-scope S3 buckets (attempts to delete S3 buckets would require users to multifactor authenticate first). 3. Observe whether live attempts to alter log data generate timely alerts to the responsible departments or individuals. 4. Obtain and inspect alarm configuration, noting: • Events and thresholds triggering the alarm (success and failure) • Recipients of the alarm are the intended departments or individuals				
Setting Log Retention		The enterprise ensures that its log retention practices meet compliance requirements as well as business needs.	The enterprise establishes minimum requirements for retaining log data, based upon defined requirements. Periodic reviews confirm alignment of current practices with the enterprise's defined log data retention requirements. Note: Required retention periods may be based upon regulations and/or determined on an application-by-application basis, depending on number of logging repositories used. Logs should be retained for a period that will allow logs to be useful in the event of security breaches or fraud investigations.				1. Determine whether logs are retained in accordance with enterprise requirements by reviewing life cycle configuration policies for logging repositories. 2. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine whether requirements exist that specify period of log retention prior to logs being purged from the environment.				

Reviewing Logs for Events of Interest		The enterprise routinely improves security posture and logging capabilities through formalized reviews.	The group or individual(s), identified by the enterprise, review logs on a periodic basis for suspicious events or anomalies. Note: Active or past security breaches may be detected through a manual or semimanual log-review process. These reviews may further identify security control weaknesses that the enterprise should mitigate for enhanced protection.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine whether procedures are in place (or automated mechanisms exist) to review logs generated by AWS applications. 2. Determine how identified anomalies or suspicious events are investigated, documented, communicated and remediated within the enterprise. 3. Obtain and inspect completed log reviews evidencing that they occur as required by the enterprise. 4. Document population of identified suspicious events and/or anomalies. Through judgmental sampling, determine whether identified suspicious events and/or anomalies have been properly investigated, documented, communicated and remediated, as necessary.				
Managing Logging Failure		The enterprise identifies and addresses logging failure events in a timely manner.	CloudWatch alarms are configured to notify the appropriate group or individual(s) when logging functionality is compromised. Note: Logging failure covers a variety of events from running out of available disk space to intentional or accidental disabling/modification of configurations. These scenarios and others should be investigated.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine the mechanism used by the enterprise to detect logging failures and the individuals who are informed of logging failures. 2. Observe generation and receipt of messages for instances where logging is disabled (or configuration modifications have disabled logging). 3. Obtain and inspect event monitoring and alarm configurations to determine whether alarms will be sent to appropriate personnel following logging failures.				
Accurate Log Timestamps		The enterprise maintains log integrity by using an authoritative and synchronized time source.	The enterprise configures EC2 instances to synchronize time with AWS Network Time Protocol (NTP) servers. Note: A majority of AWS services, like S3, Redshift, Lambda, etc., sync time with NTP servers in Amazon data centers, for which AWS will likely not provide configuration evidence. In this case, in order to gain assurance on synchronized time, the assessor may wish to leverage AWS Artifact to obtain and review SOC reports issued by AWS for those regions (and/or availability zones).				1. Interview responsible and/or accountable personnel to determine how unified timestamping is achieved for EC2 server instances deployed in the enterprise, and how often authoritative NTP server polling occurs. 2. Document the population of EC2 instances that exist in every VPC, per region. For Windows® Servers in each VPC: a) Open the Command prompt. b) Type "w32tm /query /configuration" (Amazon's time server "169.254.169.123" should be listed as the "NtpServer" value) c) Type "w32tm /query /status" to determine the polling interval for each EC2 instance. For Linux® Servers in each VPC: a) Obtain and inspect the chrony.conf file from the following directory (/ etc./chrony.conf), and determine if AWS time server is present in the file. - issue" $ chronyc sources -v " command b) Obtain and inspect screenshots that the chrony service is running on the instance and is set to run at instance startup - issue " $ sudo chkconfig chronyd on " command				
Assessing Adequate Logging Coverage		The enterprise routinely assesses completeness and accuracy of logging as the enterprise expands or contracts its IT footprint.	On a periodic basis, the enterprise reviews logging and monitoring capabilities to determine if additional logging is required or if monitoring should be disabled. Note: In AWS, there is typically a cost associated with configuring monitoring and logging solutions that the enterprise uses for its services. The enterprise should consider its monitoring needs as it onboards additional applications or resources into AWS, and as it retires them. These exercises aim to reduce white noise and manage costs.				1. Interview responsible and/or accountable individuals to determine the approaches that the enterprise takes to rightsize its logging and monitoring capabilities. 2. Inquire about: • The frequency of monitoring reviews • Documentation and communication of monitoring reviews • How decisions are made to add or remove monitoring and by whom • Timeliness of making adjustments (monitoring additions or removals) 2. Obtain and inspect completed monitoring reviews to determine whether they are occurring as required by the enterprise. 3. Obtain documentation of the population of monitoring changes in the period under review. Through judgmental sampling, obtain and inspect documented changes, to determine whether proper authorization of monitoring changes has been provided prior to executing the changes.				
Detecting Attempted Privilege Abuse		The enterprise maintains integrity over privileged network accounts by monitoring AWS account or access-rights abuse and responding in a timely manner.	CloudWatch alarms are configured to detect and inform the appropriate group or individual(s) when authentication failures occur for sensitive accounts.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine whether the enterprise has developed and deployed mechanisms that detect attempts to authenticate to privileged network accounts. 2. Inquire into the history of these types of events. Identify recipients of alerts and timeliness of responses to events. Events may include, but are not limited to: • Attempts to add inappropriate users to access roles or groups not part of their job responsibilities • Removal of appropriate users from access roles or security groups • Repeated failures to authenticate to an account over short and long periods of time • Modifying the list of APIs that a given access role or group possesses 3. Obtain and inspect alarm configuration for each scenario to determine whether triggers, receipt of alarms, and follow-up investigations occurred as required by the enterprise.				

Amazon Web Services® (AWS®) Audit Program
Security Incident Response

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/ Fail	Comments
Maintaining the Plan		The enterprise ensures that there is clear understanding across the organization regarding strategy and plan of action in the event of a security event.	Security incident response documentation is continuously updated as the enterprise evolves. Management reviews the security incident response on a predetermined basis or as needed, following operational changes.				1. Interview responsible and/or accountable individuals (security, infrastructure, executive management, etc.) to determine the specific security incident response documentation that is in scope for review and the frequency of review. 2. Inquire about methods for providing input to security incident response documentation. Understand which specific individuals provide input to the security incident response process, including those who must approve any changes or updates. 3. Obtain and inspect security incident policies, plans and procedures, and determine whether they: • Require documentation of a review by appropriate individuals • Have been reviewed within the timeframe stipulated by the enterprise • Include a summary of policy/plan/procedure changes (if any)				
Practicing the Plan			The enterprise prepares for security threats through a variety of simulated exercises. The enterprise schedules security table top exercises on a frequency predetermined by the enterprise to improve security incident response capabilities.				1. Interview responsible and/or accountable individuals (security, legal, etc.) to determine the: • Frequency of incident response practice scenarios conducted by the enterprise • Personnel involved • Scenarios practiced in relation to company operations and utilized technology 2. Obtain and inspect summary exercise reports, meeting minutes or updates to the security incident response plan resulting from tabletop exercises.				
Crisis Communications		The enterprise expressly considers and incorporates public relations into its security posture and documentation.	The enterprise has developed crisis-communication procedures that inform personnel how to report security breaches to regulators, law enforcement or customers, if necessary. Note: The enterprise should know when, how and to whom it should report security incidents (whether short-lived or prolonged). A single poorly managed security incident can put the company out of business or permanently harm its reputation. Crisis communication procedures that are reviewed and practiced over time may help reduce the risk.				1. Interview responsible and/or accountable individuals (security, legal, operations management, etc.) to determine whether security incident response policies, plans or procedures inform the enterprise: • How to identify and declare a formal crisis within the enterprise (e.g., if a security breach leads to millions of exposed PII records) • Which individuals must be included in crisis communications and how to contact them, responsibilities of other individuals across the enterprise • What approaches and requirements are necessary when speaking with the media (this may be needed for standard employees as well) • What approaches and requirements are necessary when communicating crisis information to authorities • What approaches and requirements are necessary when communicating crisis impacts to customers or internal employees (as appropriate) 2. Obtain and inspect security policies, plans and procedures, and determine whether they define and/or contain appendices describing how enterprisewide security crises should be handled. 3. Inspect the crisis communications to determine whether they are routinely reviewed for completeness and accuracy.				
Enterprisewide Visibility Through Automation		The enterprise ensures effectiveness of its security incident response program through strategic communication.	Enterprise security personnel are informed about security events of interest in a timely manner. The enterprise has deployed a security information and event monitoring (SIEM) capability to report potential security events to appropriate personnel.				1. Interview responsible and/or accountable individuals to determine which security tools (e.g., firewalls, IDS, IPS, antivirus, etc.), and event types from these tools, are feeding into the security event information management (SIEM) tool. 2. Inquire about: • The required or intended recipients of alerts generated by the SIEM • How maintenance of SIEM event monitoring is performed to update and include new event sources or remove old event sources • How event correlation between different sources is performed and achieved • How false positives, false negatives and other noise are reduced 2. Obtain documentation of the population of event sources and types managed by the SIEM. Through observation and judgmental sampling, determine whether alerting capabilities function as intended and inform the appropriate personnel. 3. Obtain and inspect completed maintenance reports or communications illustrating the enterprise's attempts to keep the SIEM in an optimal state.				
Centralized & Secured Storage of Security Events		The enterprise maintains integrity over security events by utilizing a secure incident handling application.	Enterprise security incidents are maintained within the application defined by the enterprise and are retained for the period of time determined by the enterprise. Note: It is not uncommon for certain phases of a security incident to be handled in different applications or network directories. For example, the security incident may be initially documented, investigated and eradicated in the enterprise's help desk ticketing system (e.g., ServiceNow®, Remedy®, etc.), and then investigated for root cause, using less formal means outside of that system (e.g., via meetings, word documents and reports stored in secured network directories). This may be done to keep the details of a security breach suppressed for security purposes or until necessary details of the incident are known.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine the applications or mechanisms employed by the enterprise to document investigation, resolution and lessons-learned activities resulting from security events. 2. Inquire about: • Reported events or network alerts that should drive creation of security incidents in the enterprise-designated application • Individuals with read and modify access to security incident information and how appropriateness of access is determined • Level of required detail recorded for security events (enterprises may use obscure code words to internally communicate that security events have occurred, or are occurring, and may require that minimal details be recorded in security incident tickets) • Retention requirements for security incidents and how deletion of records occurs or is triggered • Personnel access to security incidents and how routinely access is reviewed to ensure that it remains appropriate 3. Obtain and inspect management review of access listings to security incident applications or other network sources and inquire with management on appropriateness of access, if necessary 4. Document the population of security events and incidents that have occurred in the period under review. 5. Through judgmental sampling, obtain and review security incident tickets to determine whether: • Security incidents were appropriately generated or opened for security events reported • Appropriate detail is contained in the security incidents as required by the enterprise (e.g., title, reporter, date, status, etc.) • Deletion of archived security incidents is occurring as required by the enterprise				

Amazon Web Services® (AWS®) Audit Program Security Incident Response											
Process Sub-area	***Ref. Risk***	***Control Objectives***	***Controls***	***Control Type***	***Control Classification***	***Control Frequency***	***Testing Step***	***Ref. Framework/ Standards***	***Ref. Workpaper***	***Pass/ Fail***	***Comments***
Communicating with External Enterprises		To ensure that the enterprise is aware of security events of interest, the enterprise collaborates with external business partners (law enforcement, vendors, etc.).	The enterprise has appropriate contact information for external business partners. On a periodical basis, the enterprise reviews and communicates necessary contact information modifications to external business partners. Note: External entities should know who to contact if it is externally discovered that a security breach is or may be affecting the enterprise.				1. Interview responsible and/or accountable individuals to determine which external parties the enterprise provides security contact information to, along with alternative enterprise contacts, how the information is provided to external parties and how often contact information is updated then shared. 2. Obtain and inspect crisis communication plans, security documentation or update communications sent to required external contacts, to determine if valid information is available for security event reporting purposes. From the AWS Management Console, in the AWS Navigation menu: a) Click on the "Account Name" logged into the AWS account. b) Click "My Account". c) Inspect the "Alternate Contacts" section. d) Under the "Security" field, ensure appropriate enterprise contact details are populated.* *Center for Internet Security®, *CIS Amazon Web Services Foundations* , CIS Benchmarks™, v1.2.0, 23 May 2018, *https://www.cisecurity.org/benchmark/amazon_web_services/*				
Creating Roles to Manage AWS Incidents		The enterprise ensures that there is role-specific plan of action in the event of a security event.	The enterprise creates appropriate access roles for external AWS support personnel assisting with security incidents. The enterprise has created an AWS Support role and managed policies that limit access to AWS applications. Note: If the enterprise has a paid support plan with AWS, an IAM access role should be created and managed that provides only the necessary access for AWS support personnel to access the environment. This may be limited to incident response assistance or other support defined by the enterprise				1. Interview responsible and/or accountable individuals (operations management, security , etc.) to determine the number of IAM roles that exist to provide external support personnel access to the environment and the access permissions granted to each role. 2. Inquire about: • Frequency of review for AWS Support roles and related permissions • Users in the enterprise that can create or modify AWS Support roles • Level of monitoring in place that detects and informs the enterprise when AWS Support roles are used, created or modified 3. Obtain and inspect AWS Command Line Interface output that filters for the "AWSSupportAccess" managed policy value (aws iam list-policies --query "Policies[?Policy Name == 'AWSSupportAccess']"). 4. Determine which users, groups or roles the policy is attached to and whether this is appropriate. Appropriateness can be determined through inspection of the associated Amazon Resource Names (ARN) that the policy attaches to (aws iam list-entities-for-policy --policy-arn <iam_policy_arn>). 5. Inspect each managed policy for appropriateness of permissions detailed in the policy statements				

Amazon Web Services® (AWS®) Audit Program
Data Encryption Controls

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/ Fail	Comments
Defining Encryption Requirements		The enterprise applies appropriate encryption to individual data stores that is commensurate with business requirements	The enterprise requires a minimum of AES 256-bit level encryption for data at rest and in transit.				1. Interview responsible and/or accountable individuals (security, operations management, etc.) to determine minimum levels of encryption that have been defined and documented for each AWS application in use and related resource(s). Further inquiry should determine: • Existence and location of encryption requirements • Individuals or departments to whom the requirements are communicated • Frequency and methods used to assess compliance against the requirements • Automated mechanisms in place used to validate compliance or inform personnel of potential noncompliance 2. Obtain and inspect documented encryption requirements defined by the enterprise to determine if all AWS applications in use are included.				
Encrypting Data by Classification		The enterprise maintains data confidentiality through the application of encryption, as defined by data classification requirements.	The enterprise secures AWS data containers (S3 buckets, RedShift clusters, etc.), using client-side and server-side encryption.				1. Interview responsible and/or accountable individuals (security, operations management, etc.) to determine types (AES, TLS, etc.) of encryption that are applied based upon business-defined data classifications or other requirements for AWS applications. (May have been covered in previous interview. If not, proceed as follows.) 2. Obtain and inspect encryption settings for in-scope AWS applications and related resources. The following list contains some examples (but may not include specific containers) of interest to the assessor: Simple Storage Service - S3 From the AWS Management Console, access the S3 service: a) Click on individual S3 buckets of interest. b) Click the "Properties" Tab). c) Inspect the "Default Encryption" property (None or AES 256). Dynamo Database - Dynamo DB creates data at rest protection if default settings are selected when creating a table From the AWS Management Console, access the DynamoDB service: a) Click the "Dashboard" option under "Tables". b) Select the Dynamo tables of interest. c) Click the "Overview" tab to access resource details. d) Check the "Encryption" configuration property (Disabled or Enabled). Redshift - Data at Rest From the AWS Management Console, access the Redshift service: a) Click "Clusters". b) Select Redshift clusters of interest and navigate to the cluster database properties. c) Verify the "Encrypted" property (Yes or No).				
Securing Remote Connectivity		The enterprise maintains data confidentiality and integrity for external network sources and destinations.	The enterprise requires encrypted connections for communications with external destinations.				1. Interview responsible and/or accountable individuals to determine (development, operations management, infrastructure, etc.) which AWS applications and related resources allow, or are configured to accept, external or public web connectivity. Further inquire which publicly facing AWS applications and related resources contain, process or transmit sensitive data. Some examples include: - AWS Redshift - AWS CloudFront Distributions - AWS S3 2. Obtain and inspect SSL settings for in-scope AWS applications and related resources: Redshift From the AWS Management Console, access the redshift service: a) Click "Clusters". b) Click the cluster(s) of interest. c) Click the "Configuration" tab, then "Cluster Properties" , then "Parameter Group". d) Under the "Parameters" tab, inspect the "require_ssl" property (True or False). CloudFront Distributions From the AWS Management Console, access the CloudFront Service: a) Click "Distributions" then the individual distributions of interest. b) Click "Distribution Settings" then the "General" Tab. c) Examine the "Security Policy" property. A value other than "TLSv1" or "TLS_2016" should be present. If either option is present the default CloudFront certificate may be selected for use (which is insecure, as TLS1.0 is exploitable). Inquire further to determine whether these security policies are present. Simple Storage Service - S3 From the AWS Management Console, access the S3 service: a) Inspect the buckets of interest, then the "Permissions" tab. b) Click the "Bucket Policy" and inspect the listed policy configuration. c) For any policies that allow a given resource access to the bucket in question, a false statement should be in effect if clients accessing the bucket do not have SSL transport set to "TRUE".				
Detecting Misconfigured Encryption		The enterprise maintains integrity of encryption status through use of monitoring.	The enterprise has developed capabilities to identify and respond to encryption failures or misconfigurations in a timely manner.				1. Obtain documentation of the population of CloudWatch events configured for each in-scope AWS application and related resource with specific attention to monitoring encryption status (at rest and in transit). Through judgmental sampling, obtain and inspect CloudWatch alarm configuration to determine: a) Whether changes to AWS application encryption status will generate alerts (SNS topics) b) To which department or individuals the alarms are sent 2. From a judgmental sample of triggered alarms, determine timeliness of response. 3. Determine how the alarming capability is maintained as AWS applications change or as new applications are introduced.				

Amazon Web Services® (AWS®) Audit Program
Logical Access Controls

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/ Fail	Comments
Securing Root Account Access		Accountability and security of AWS-based business functions are achieved through restricted access to AWS root accounts.	The enterprise disables AWS root account access and utilizes a secured password vault to control use of account credentials. Note: The AWS root account is an anonymous super-user account that cannot be restricted. Best practice is to disable access keys associated with these accounts and password-vault the associated password, granting access only on a restricted, need-to-know basis. There is a single root account for every individual AWS billed account.				1. Interview responsible and/or accountable individuals (security, operations management, infrastructure, etc.) to determine the methods used to secure and restrict the use of AWS root accounts that exist in the environment. 2. Inquire about: • Potential instances where root account usage may be required • Historical or actual instances where root account usage was required and subsequently utilized • Where the associated root account password is stored (network directory, physical/electronic password vault, etc.) • How use of the account is requested, approved and documented if usage is necessary • Monitoring used to track individuals who view or may attempt to access root account passwords • Whether AWS access keys are currently enabled or disabled for root accounts 2. Obtain and inspect the AWS credential report for individual AWS root accounts. From the AWS Management Console, access the Identity & Access Management (IAM) service: a) On the left hand side of the screen, click "Credential report" then "Download Report" b) Inspect the row for the user <root account> with specific attention to the following items: "password enabled", "password last used", "Access Key 1 Active", "Access Key 1 Last Rotated", "Access Key 1 Last Used" c) Repeat access key validations for access key #2. 3. Obtain and inspect password vault access lists and inquire with management on their appropriateness; further determine whether views or modifications of the password are logged.				
		The enterprise maintains integrity of AWS root accounts by implementing multifactor authentication.	AWS root accounts are configured to require multifactor authentication before they may be used.				1. Interview responsible and/or accountable individuals (security, operations management, infrastructure, etc.) to determine types of access protections applied to AWS root accounts and individuals with access to enable or disable these protections. 2. Obtain and inspect access protections applied to AWS root accounts: From the AWS Management Console, access the Identity & Access Management service: a) Review the "Security Status" pane; the console will inform the user if multifactor authentication is enabled for the root account. b) Alternatively, on the left-hand side of the screen, click "Credential Report" then "Download Report". c) Review the status of the "mfa_enabled" column for the <root account> user.* *Center for Internet Security®, *CIS Amazon Web Services Foundations* , CIS Benchmarks™, v1.2.0, 23 May 2018, *https://www.cisecurity.org/benchmark/amazon_web_services/*				
Establishing Role-based Access		Data confidentiality is ensured by managing access based on the level of access needed for users or network functions to perform their intended roles.	The enterprise has developed and configured access roles to provision users or network services according to the principle of least privilege. Note: There can be hundreds of identity and access management (IAM) roles and even more permissions policies. For the sake of timely testing, the assessor may wish to focus on users, groups or access roles that provide privileged access, such as a system administrator or network administrator.				1. Interview responsible and/or accountable individuals (security, infrastructure, operations management, etc.) to determine how enterprise users are provided access to AWS applications and related resources. 2. Inquire about: • Existing IAM users that are not part of any IAM access group or role, along with justification, if necessary • Level of documentation that exists for desired access groups, roles and permission policies (i.e., ask whether desired access documented is) • How permission policies are developed, approved and attached to IAM access groups or roles (for new or modified groups or roles) • Individuals responsible for creating or removing IAM users, groups, roles and attaching permission policies to IAM groups and roles • How least privilege is achieved and maintained for individual IAM access groups, roles and permission policies • How privileged and nonprivileged access groups, roles and permission policies are identified and maintained 3. Obtain documentation of the population of: • IAM Users • IAM Groups • IAM Roles • IAM Permission Policies 4. Through judgmental sampling, obtain and inspect IAM permission policies that are attached to individual IAM users, access groups and roles. Inquire further with management on appropriateness of permissions associated to individual roles included in the sample. Alternatively, the assessor may use management documentation that describes the permissions a given user, group or roles should possess and inspect the applied permissions directly using the IAM management console.				
Segregating Duties		The enterprise maintains the integrity and confidentiality of AWS applications through identification and reduction of conflicting access.	The enterprise has developed network-access baselines based on position responsibilities and generates alerts when modifications occur. Note: Examples of potential access conflicts include: • Software developers who have access to environments or toolsets allowing code deployments to production • System or network administrators who have full access to logging repositories or configurations				1. Interview responsible and/or accountable individuals (HR, security , operations management, etc.) to determine the approach the enterprise uses to prevent, detect and correct potential segregation of duties conflicts. 2. Inquire about: • Documentation used to record undesired combinations of access by environment, department, job role or business function • Mechanisms used to authorize and monitor changes to AWS access roles and associated permissions • Frequency of review that occurs for changes in access or new applications that introduce potential access conflicts 2. Obtain and inspect segregation-of-duties access matrix to determine if the enterprise has completely identified and documented undesirable access combinations for its work force. 3. Obtain and inspect IAM groups, roles and permissions policies to determine if segregation of duties conflicts exist that are noncompliant with enterprise requirements. 4. Observe (or obtain) and inspect alarms or alerts that notify personnel to access conflicts that occur in the environment through permissions policy modifications.				

Amazon Web Services® (AWS®) Audit Program
Logical Access Controls

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/ Fail	Comments
Restricting Administrative Toolsets		The enterprise maintains confidentiality and integrity of the environment by limiting administrative tools available to personnel.	The ability to administer AWS applications is limited to authorized tools and users. Note: A variety of administrative tools are available to personnel who can administer the environment, including, but not limited to, the following: • AWS command-line interface • AWS Management Console • Microsoft® PowerShell® • Software development kits				1. Interview responsible and/or accountable individuals (security, infrastructure, operations management, etc.) to determine how enterprise personnel are authorized and provided access to enterprise approved administrative tools. 2. Inquire about: • Users that can generate IAM access key to authenticate tools (composed of 2 parts, an access key ID and a secret access key) • The tools that are allowed for environmental administration • The tools that are not allowed for environmental administration • Methods used to identify use of noncompliant administrative tools • Methods in place to ensure personnel are using secure or current versions of administrative tools • Method of maintaining secure access to administrative tools • Tools authorized by department or job function (i.e., developers should only have software development kit access, for example) 2.Obtain and inspect a list of administrative users within the environment (system administrators, network and server administrators, etc.), along with a list of approved toolsets for each user. 3. Obtain and inspect tools assigned to IAM users: From the AWS Management Console, access the Identity & Access Management (IAM) service: a) Click "Users" then inspect the "access key age" column. Any values other than "none" indicate the user possesses valid access keys which must be supplied to either the command-line interface during installation, or to various software development kits (JavaScript, PHP, Ruby, etc.). Additional inquiry regarding whether individual users have installed are using SDKs to access or manipulate AWS applications will be required. b) Further inspect the "Console Access" columns to determine if the user has AWS Management Console access. The corresponding "password" column indicates age of the user's password. PowerShell® requires valid AWS account credentials to access AWS applications. Users can insecurely store credentials directly within scripts or in 1 of 2 credential stores on their workstation in the following locations. The assessor can choose to observe or inspect these locations for users of interest: • The AWS SDK store, which encrypts credentials and stores them in user's home folder. In Windows, this store is AppData\Local\AWS Toolkit\RegisteredAccounts.json • The credentials file, which is also located in the user's home folder, but stores credentials as plain text.				
Removing Access		Once identified, inappropriate access (e.g., access that no longer serves a business need) is completely removed in a timely manner.	AWS accounts are disabled after an enterprise-defined period of inactivity, then are removed, if necessary.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine the mechanisms used to identify and disable inactive accounts. 2. Document the population of in-scope users for the period. 3. Obtain and inspect screenshots demonstrating that IAM users and/or associated access keys are deactivated following the enterprise-defined period of inactivity.				
Segregating Duties		The enterprise ensures data confidentiality and security through password protection of user accounts accessing AWS applications.	The system enforces password policies which: • Require minimum password length • Constrain use of historical passwords • Require predefined password complexity				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine the number of distinct user populations which exist to access the environment, password requirements for each population and how password requirements are enforced against each population of users (federated users that access AWS from the enterprise environment, IAM users, etc.) 2. Obtain and inspect the password policy for each user population: For IAM users: From the AWS Management Console, access the Identity & Access Management (IAM) service: a) Click "Account Settings" and inspect the: - Minimum password length - Complexity settings (confirm that password requires one upper-case letter, one lower-case letter, number and nonalphanumeric value) - Enable password expiration and associated value. - Prevent password reuse and associated value of passwords to remember. For federated users: Obtain and inspect default domain-password policy to determine if it meets complexity, password age, history and length requirements.				
Assessing Access Roles & Permissions		The enterprise maintains appropriateness of access roles and related permissions policies through ongoing reviews and real-time monitoring.	Amazon CloudWatch alarms are configured to alert the appropriate enterprise-defined department or individuals when AWS access roles or permissions are created or modified. Management reviews appropriateness of access provided to AWS access roles and associated permissions on a regular basis, as defined by the enterprise. Note: Real-time events related to creation or modifications to access roles and their permissions should focus on privileged groups such as system administrators or domain administrators. Modifications to these groups may indicate a network attack. Additionally, management or responsible individuals should conduct annual reviews of roles (regardless of any triggered monitoring alerts) to ensure that permissions associated to access roles serve valid business needs and do not allow inappropriate access.				1. Interview responsible and/or accountable individuals (security, infrastructure, operations management, etc.) to determine the approaches or mechanisms used by the enterprise to detect creations or modification events related to IAM users, groups, roles or permission policies. 2. Inquire about: • Specific users, groups, roles or permissions policies that are in scope • Individuals who are informed of creation or modification events for in scope items • Timeliness of response • History of these events and impacts • Frequency of management review, documentation and approvals for IAM users, groups, roles and permissions policies 2. Obtain documentation of the population of in-scope users, groups, roles and permissions policies that are monitored. Through judgmental sampling, obtain and inspect configured event alarms noting the conditions triggering alarms and recipients of alarms. 3. Obtain documentation of triggered alarms in the period. Through judgmental sampling, obtain and inspect documentation demonstrating that the alarms were sufficiently investigated by responsible individuals. 4. Obtain and inspect completed management reviews demonstrating that IAM users, groups, roles and permissions policies were completely reviewed for appropriateness, and that noted removals identified by management were processed in a timely manner.				

Amazon Web Services® (AWS®) Audit Program
Logical Access Controls

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/ Fail	Comments
Delegating Access to External AWS Accounts		The enterprise enforces AWS application confidentiality and integrity by requiring multifactor authentication.	Privileged users and application programming interfaces (API) are required to authenticate to the network using multifactor authentication (MFA). Note: Validating API MFA may be done a variety of ways. The validation outlined under the testing step, "Validating MFA for APIs," reflects basic validation and only applies to AWS applications that can use temporary credentials.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine whether users and application programming interfaces (API) must supply additional credentials before they may interact with AWS applications and related resources. 2. Inquire about: • In-scope users and APIs • Method and when additional authenticators are enforced (e.g., during user creation, after API deployment, etc.) • Individuals responsible for configuring and enforcing multifactor authentication (MFA) • Types of MFA devices or configurations that are used to secure user access and APIs 3. Obtain documentation of the population of in-scope users and APIs. Validating MFA for users: From the AWS Management Console, access the Identity & Access Management (IAM) service: a) Click "Users" then inspect the "MFA" column (Enabled or Not Enabled) Validating MFA for APIs: a) Document the population of users that are required to have an issued MFA device for in-scope API operations requiring MFA for API. b) Through judgmental sampling, obtain the permissions policies attached to the user and inspect the policy for the following policy condition for each in-scope API: 1) Condition: "Bool" : { "aws:MultiFactorAuthPresent" : "True" } This requires the API referenced in the Action section of the policy to MFA the associated user before the API may be used.				
		Management of external access to AWS applications through authorization ensures that actions taken are restricted to actions that have been approved for that particular role.	The enterprise creates and manages identity and access management (IAM) roles that external enterprises use to access AWS applications and related resources. Access is terminated in a timely manner when there is no longer a business need for the access.				1. Interview responsible and/or accountable individuals (operations management, vendor management, security, etc.), to determine the number of external enterprises and AWS accounts that are allowed access to the AWS environment. 2. Inquire about the: • Exact method used to authorize, provide or delegate access (typically through an AWS IAM role solely controlled by the enterprise) • Types of permissions granted to external enterprise accounts • Individuals responsible for provisioning and communicating external AWS access • Frequency for reviewing appropriateness of connection and timeliness of removal (should business relationships change) • Monitoring of account usage (for example, AssumeRole API calls, along with associated principal identifiers, can be used to track usage) 3. Obtain documentation of the population of external enterprises and associated roles with access to the AWS environment. Through judgmental sampling: a. Obtain and inspect related permissions policies attached to the roles and inquire with management on appropriateness of access. b. Obtain and inspect completed authorization forms and management reviews of external enterprise access.				
Controlling Access to Cryptographic Keys		The enterprise maintains confidentiality and integrity of cryptographic information by restricting access to appropriate individuals.	The enterprise grants AWS Key Management Service (KMS) access to personnel (based on job responsibilities) and implements access based on the principle of least-privileged. The enterprise utilizes Amazon CloudTrail® to monitor AWS KMS API calls for appropriateness. Note: When using KMS, enterprises can control access by defining a resource-based policy known as the default key policy.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.), to determine which users or departments are responsible for managing access to the enterprise's cryptographic key-management services. 2. Inquire about: • The number of cryptographic keys that exist and what data are they meant to protect • Any cryptographic keys stored offsite with another provider and justification • How key policies are developed and applied to keys • How access is authorized and how frequently access is reviewed for appropriateness • Individuals with authority to change key policies • Existence of monitoring to generate alerts if key policies are modified 2. Obtain documentation of the population of KMS Customer Managed Keys (CMK) and associated default key policies. Through judgmental sampling: a. Obtain and inspect default key policies with specific attention to the principals and the actions each principal is allowed to take in order to determine whether they meet enterprise-defined access requirements. b. Obtain and review configuration of monitoring alarms to determine whether capabilities exist to alert appropriate personnel of inappropriate actions (e.g., copy or delete actions).				
Enforcing Session Timeouts		The enterprise ensures integrity of AWS application sessions by enforcing session timeouts.	AWS user sessions time out after an interval defined by the enterprise. Note: This interval can span from 1 to 12 hours, and is controlled by the AWS Security Token Service.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.), to determine how long user sessions should persist (i.e., how long user sessions remain active), after becoming inactive. 2. To validate AWS-user session-timeout values: From the AWS Management Console, access the identity and access management (IAM) service. a) Click "Roles" then inspect the "Max CLI/API Session" column value. b) Alternatively, the assessor may ask a given IAM user to login, mark the time they accessed the console or command-line interface then wait for the time specified to determine if a timeout occurs and forces reauthentication.				
System Use Notifications		The enterprise ensures security and appropriate use of its network by defining and communicating expected behavior to users prior to granting user access.	A system-use notification, outlining acceptable use, is presented to users and requires their acknowledgement before they are granted AWS application access.				1. Interview responsible and/or accountable individuals to determine whether a system notification is presented to users who are attempting to access AWS applications and related resources. 2. Obtain and inspect an example of centralized configuration, demonstrating that the notification is presented to all users, and requires their acknowledgment, before users are allowed to proceed with AWS applications or related resource access.				

Amazon Web Services® (AWS®) Audit Program
Asset Configuration and Management

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/ Fail	Comments
Utilizing Baselined AWS Resources		Assurance that operational requirements for security or other purposes are met is gained through a formal process for deployment of AWS applications in the environment.	The enterprise utilizes AWS CloudFront templates to develop and deploy AWS applications in the environment. The enterprise routinely assesses adequacy of CloudFront templates to ensure that they meet business requirements for security and/or functionality. Note: The enterprise can leverage CloudFront templates to baseline AWS application resources (e.g., S3 buckets, EC2 instances, etc.) and configurations that meet certain requirements (e.g., that S3 bucket logging is enabled by default, or client-side encryption is enabled). These templates can be further leveraged to continuously delete and regenerate the entire AWS environment on an enterprise-defined frequency, which is a good security practice, and ensures that minimum baselines are constantly achieved.				1. Interview responsible and/or accountable individuals to determine how the enterprise develops and deploys individual applications and related resources (assets) within the environment. Expressly consider how the enterprise sets, monitors and ensures minimum security requirements for assets. 2. Inquire about the specific configurations or security requirements each in scope AWS application should meet as set forth by the enterprise and document these requirements per AWS application asset. 3. Obtain documentation of the population of AWS application assets that utilize CloudFront templates for asset generation and security configuration. 4. Using a judgmental selection, obtain and inspect samples of AWS applications to determine whether the CloudFront template adequately sets the required configurations or security requirements. 5. Using a judgmental selection, obtain and inspect evidence of reviews demonstrating that the enterprise assesses adequacy of asset configurations or security configuration provided by individual CloudFront templates.				
Change Management		The enterprise expressly authorizes changes to AWS applications and related resources to ensure that any modifications are appropriate and support business needs.	AWS asset configuration modifications are formally documented, reviewed, tested and approved, prior to production deployment.				1. Interview responsible and/or accountable individuals to determine whether processes and procedures are in place that control modifications to AWS application and related resources (assets). Review the population of applications and related resources the processes and procedures apply to. Review which individuals are responsible for each part of the change-management process. 2. Document population of changes that occurred during the period under review. 3. Through judgmental selection, obtain and inspect change records to determine if the process was followed, as documented in the process/procedures.				
		The potential risk that changes in the environment adversely affect operations is mitigated through monitoring of AWS assets.	The enterprise utilizes monitoring solutions that provide detailed records of asset modifications. Modifications are retained for a sufficient amount of time. AWS Config records asset changes in designated CloudWatch events and S3 buckets, including: date of the change, the account making changes, results of the change and additional information supporting appropriateness of the change.				1. Interview responsible and/or accountable individuals to determine how the enterprise logs modifications to in-scope AWS applications and related resources (assets), and which assets are in scope. Inquire about: • The level of detail captured by the monitoring solution • Where records are sent • How long they are retained • Individuals with access to read/review any changes 2. Document the AWS CloudWatch events and rules that are configured to capture AWS asset modifications. 3. Document the AWS S3 bucket(s) where change modifications are recorded. 4. Using evidence from the previous test, review a sample of asset changes that occurred in the period. 5. Determine whether record of the change was documented by the appropriate CloudWatch event, stored in the associated S3 bucket and included sufficient detail as required by the business. 6. Examine retention periods for the change records to ensure they will be available if needed during an investigation. (Verify In the AWS S3 dashboard: click the bucket of interest, click the "Management" Tab, then the "Lifecycle" subtab).				
		The enterprise maintains the environment's integrity by establishing change schedules.	The enterprise has designated time periods for requested changes by priority and requires additional review and approvals for emergency changes. Note: Establishing change schedules based on priorities helps reduce enterprise chaos caused by change, and also facilitates identification of inappropriate changes.				1. Interview responsible and/or accountable individuals to determine if formal time periods have been designated for changes based on their enterprise designated priority (1, 2, 3, etc.). 2. Determine whether additional reviews and approvals are required for emergency changes that may occur. 3. Determine which individuals are responsible for reviewing and approving emergency changes. 4. Review the difference in volume between standard and emergency changes (i.e., are personnel abusing the emergency change process by declaring normal changes as emergencies? This can typically be identified by reviewing the total population of changes and examining percentage of change categorization.) 5. Through judgmental selection, determine whether completed changes are being implemented during the designated time periods.				
Identifying and Remediating Asset Vulnerabilities		Potential risk regarding AWS application and related resource vulnerabilities is mitigated.	The enterprise performs vulnerability assessments through the use of scans using enterprise-identified tools and on an enterprise-determined frequency. Note: This control may be achieved through a variety of tools, such as CloudCheck, Netsparker or other tools provided by AWS. It may also involve manual checks via self-assessments or external audits.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine methods and/or frameworks used by the enterprise to identify, document and remediate vulnerabilities in AWS applications and related resources (assets). 2. Determine who has access to vulnerability scanning tools, how output of scanning tools is interpreted and prioritized within the enterprise, and the degree and timeliness of remediation performed when vulnerabilities are discovered. 3. Document the population of vulnerability scan outputs. 4. Through judgmental selection, determine whether identified vulnerabilities have been remediated within the allowable timeframes stipulated by the enterprise.				
External Penetration Testing		Potential security weaknesses are identified through penetration testing.	The enterprise schedules and performs penetration testing in accordance with its predetermined frequency to identify and remediate vulnerabilities. The enterprise contracts with external subject matter experts to identify and remediate AWS asset vulnerabilities in a timely manner.				1. Interview responsible and/or accountable individuals (security, infrastructure, etc.) to determine vendors, type (black box/white box, etc.), frequency and resources devoted to conducting penetration testing exercises. 2. Inquire about: • Individuals involved in setting the statement of work • How nondisclosure of vulnerabilities is handled • Individuals or departments within the organization that receive the final report • Responsibilities and timeliness for resolving identified vulnerabilities (confirmed, internally reviewed, assigned, etc.) 3. Obtain and inspect penetration testing statements of work, schedules and final-report summaries (if available) to determine whether penetration testing exercises have been scheduled and completed as discussed.				

Amazon Web Services® (AWS®) Audit Program Asset Configuration and Management											
Process Sub-area	***Ref. Risk***	***Control Objectives***	***Controls***	***Control Type***	***Control Classification***	***Control Frequency***	***Testing Step***	***Ref. Framework/ Standards***	***Ref. Workpaper***	***Pass/ Fail***	***Comments***
Identifying and Removing Unnecessary Assets		Enterprise objectives related to cost containment are supported through identification and removal of unnecessary assets in a timely manner.	The enterprise has configured AWS CloudWatch alarms to identify assets no longer serving valid business purposes. Note: Alternatively, AWS Budgets can be leveraged to identify areas where enterprises might be overspending, by setting resource thresholds that inform users when services near or exceed the thresholds. AWS typically charges customers for services they use, but there are also costs associated with services that store information no longer needed by the business. Other non-AWS tools, such as Janitor Monkey, exist to identify unused AWS assets and automatically report them.				1. Interview responsible and/or accountable individuals (operations management, infrastructure, finance, etc.) to determine methods used by the enterprise to identify AWS applications and related resources (assets) that are being charged to the enterprise but are not providing a business value. 2. Inquire about: • AWS applications and related resources (assets) that are in scope • CloudWatch alarms configured for each AWS asset • Triggers that exist for each configured CloudWatch alarm (i.e., what limits are the enterprise monitoring per asset?) • Individuals who can set or modify CloudWatch alarms and triggers • Individuals who receive alarm output, once an alarm is triggered and the mechanism delivers the message (SNS topics, etc.) • Time limits and evaluation methods to determine whether an asset is to be removed • Length of time and location where triggered alarms are stored • Conditions triggering deletion of alarm messages 3. Obtain documentation of the population of AWS assets that should have alarms configured. Through judgmental sampling, test to determine whether: • CloudWatch alarms are configured • Alarm thresholds are configured in accordance with enterprise requirements • Alarms are configured to notify the appropriate group within the enterprise • Alarms trigger once the configured threshold is crossed • Timely investigation of alarms is conducted and corrective is taken				
Defining Data Retention Requirements		The enterprise has developed data retention and purge directives for AWS assets to ensure data are retained only for the time required by law or for business needs.	Data management policies and processes exist for AWS applications to manage enterprise life cycle requirements.				1. Interview responsible and/or accountable individuals (legal, security, operations management, etc.) to determine how the enterprise defines and programmatically enforces data retention and data-purging activities for individual AWS applications and related resources. 2. Obtain and inspect data management policies. Through judgmental sampling, obtain and inspect evidence for each in-scope AWS asset demonstrating data-retention policies; archive or remove data in accordance with defined policies or documented configuration.				

Amazon Web Services® (AWS®) Audit Program
Network Configuration and Management

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/ Fail	Comments
Maintaining Security Architecture & Network Traffic Baselines		Network security architecture is baselined and supports the enterprise's security requirements.	AWS network security architecture is routinely reviewed and compared against enterprise-defined security requirements. Periodic reports are produced and sent to appropriate personnel for review. Any deficiencies are addressed in a timely manner.				1. Interview responsible and/or accountable personnel to determine whether a security network architecture standard exists and has been formally documented and applied to the environment. 2. Determine the frequency of reviews that assess compliance of the network security architecture with the documented standard. 3. Determine how compliance of the network security architecture with the documented standard is assessed (e.g., python scripts run Center for Internet Security® CIS® AWS security benchmarks daily and produce reports to security, etc.). 3. Obtain and inspect completed compliance reviews and confirm that any instances of noncompliance are remediated in a timely manner.				
		The enterprise can identify and take timely action against inappropriate network traffic.	The enterprise has deployed a security information and event management (SIEM) capability to define normal traffic patterns and report suspicious events to personnel in a timely manner. SIEM configuration and event logs are routinely assessed by the enterprise to ensure the tool functions as intended.				1. Interview responsible and/or accountable individuals (security, networking, etc.) to determine if network baselines have been established to facilitate an understanding of standard versus abnormal network behavior. Baselines may include indicators such as volume input/output, top resources or AWS applications that generate traffic on a daily basis, etc. Confirm the following: • Degree of automated versus manual capabilities that are used to define baselines, inspect traffic, record results and detect anomalies identified relative to established baselines • Retention of point-in-time baselines captured and secured for later analysis • Frequency of review used to ensure the baseline and alerting capability continues to function as intended • Timeliness of response/remediation by enterprise personnel to alerts received by the baselining capability 2. Document population of AWS application and related resources captured by the network-baselining activity by obtaining population of baseline alerts or reporting configuration for each in-scope AWS application and related resource. Confirm that baselining occurs, has thresholds configured and is monitored (either automatically or manually) by personnel. Alternatively, the assessor may request that the enterprise generate certain types of traffic to trigger threshold alarms and observe that alerts are generated and sent to the appropriate personnel.				
		The enterprise employs isolated network environments to ensure integrity of its various business operations.	Separate AWS environments have been created to facilitate production, staging, test and development functions.				1. Interview responsible and/or accountable individuals (network architecture, engineering departments, etc.) to determine number of business environments that exist (production, stage, R&D, etc.) and where these environments have been deployed within the AWS network. 2. Further determine how logical isolation of each environment is achieved, maintained and how noncompliance is detected. 3. Obtain and inspect the following for each environment, testing for uniqueness: • AWS account numbers each environment is billed under • VPC-ID • Classless Interdomain Routing (CIDR) designations • Https login URLs 4. Additional testing may focus on inspecting: • Deployed resources in each environment (EC2 or S3 bucket names, etc.) • User access (e.g., developers with access to production environment resources/applications, etc.)				
Environment Segregation		Network communications are managed through a formal network traffic-management program.	The enterprise restricts inbound and outbound AWS network traffic to interactions which serve valid business needs				1. Interview responsible and/or accountable individuals (infrastructure, networking, security, etc.) to determine the approach the enterprise takes to authorize network sources, destinations, ports, protocols, external enterprises, etc. 2. From the AWS Management Console, access the AWS Virtual Private Cloud (VPC) service and inspect the following elements for appropriateness: • Configured security groups (firewall rules) per VPC • AWS subnets that exist per each VPC and business environment (prod, stage, etc.) • Routing tables in use per subnet • Network access control lists • Internet gateways deployed and NAT configurations (servers and resources should not be publicly accessible but instead communicate through a single secured point) • Georestrictions applied to each VPC or AWS application (limiting certain IP address ranges from interacting with the AWS environment) • Configuration of subnets, security groups 3. Access of external enterprises is routinely assessed for appropriateness leading to adjustments where necessary (e.g., remove unused firewall rules, remove former business partners or extranet connections, etc.). • VPC flow logs that monitor traffic among VPCs or out to other sources/destinations				
Restricting Administrative Access		The enterprise provides privileged access to personnel in accordance with valid business need.	AWS Management tools are restricted to the department identified by the enterprise and provide personnel access based on the principle of least privilege.				1. Interview responsible and/or accountable individuals (security, operations management, etc.) to determine: • Types of administrative tools provided to enterprise personnel allowing them to access and manipulate the environment. Tool examples include, but are not limited to: a) AWS root account b) AWS Management Console c) AWS Command Line Interface (CLI) d) AWS Software Development Kits (SDKs) e) PowerShell® • Method for restricting access to each tool based on least-privilege rights/permissions (e.g., AWS access associates to specifically assigned APIs that grant rights to resources and applications) • Request and authorization process for each administrative tool • Frequency of reviewing access provided to a given tool and individuals with access to each tool 2. Document population of in-use tools, access rights/permissions and assigned individuals/access roles. 3. Through judgmental sampling, obtain and inspect administrative tool access authorizations. 4. Through judgmental sampling, obtain and inspect reviews of administrative tools access reviews.				

Amazon Web Services® (AWS®) Audit Program Network Configuration and Management											
Process Sub-area	***Ref. Risk***	***Control Objectives***	***Controls***	***Control Type***	***Control Classification***	***Control Frequency***	***Testing Step***	***Ref. Framework/ Standards***	***Ref. Workpaper***	***Pass/ Fail***	***Comments***
Maintaining Valid VPC Peering Connections		Connectivity among AWS Virtual Private Clouds (VPCs) exist solely to serve appropriate enterprise business needs.	VPC peering connections require management approval and are routinely assessed for appropriateness. Note: Peering connections can be established with external business partners who have an AWS account or established among other AWS accounts or VPCs. Peering connections should only exist for the time necessary to conduct valid business transactions.				1. Interview responsible and/or accountable individuals to determine: • Number of VPC peering connections that exist in the environment • AWS applications and levels of access granted to the peered connection • Business purpose(s) of the peering connection 2. From the AWS Management Console, access the Virtual Private Cloud (VPC) service: a) Click "VPC Peering Connections". b) Inspect the "Description" tab to understand which AWS accounts made and accepted the peering connection(s) (explicit authorization is required between AWS accounts establishing peering connections) c) Inspect "Tags" tab to determine whether the use of the peering connection is defined d) Inspect "Routing Tables" columns to determine the network sources and destinations allowed through the peering connection. Inquire further for individual routing table appropriateness. 3. Obtain and inspect routine reviews of the peering connection to ensure only valid connections remain in effect.				
Network Redundancy Between the Enterprise and AWS		The enterprise maintains availability for AWS resources that depend on enterprise-managed IT systems.	Connectivity between the enterprise and AWS is fault tolerant through use of highly available VPN connections. Note: This control is important for enterprises that federate AWS access using local Active Directory® groups or other identity stores which do not exist within AWS and translate to an AWS IAM role or Amazon Cognito® user pool. Continuous, secure and highly available connectivity between the enterprise and AWS to facilitate these functions is the focus of the control testing.				1. Interview responsible and/or accountable individuals to determine whether AWS resources rely on IT assets (e.g., servers, databases, identity stores, etc.) that are physically located on the enterprise's premises and whether these resources are required for proper functioning of the AWS resources. 2. Using the AWS Management Console, access the Virtual Private Cloud (VPC) service: a) Click "Site to Site VPN" connections. b) Inspect the number of VPN connections that are configured and where the devices are physically located: device name usually indicates city or region where the device is located. c) If a VPN connection is not highly available, the AWS "Site to Site VPN" dashboard will inform the user via onscreen message. Alternatively, the "Notifications" section of the "Site to Site VPN" dashboard can be accessed; clicking "Read Messages" will display the message, if the condition is present.				
Securely Integrating Enterprise Systems to AWS		The enterprise leverages integration to simplify operational processes to achieve its strategic objectives.	The enterprise has defined processes and procedures to integrate on premises systems and data with AWS applications and functionality. Note: There may be legacy systems or other on premises systems the enterprise cannot contractually migrate or is not willing to migrate to AWS that need security and availability controls. Testing to determine the population and general approach taken to migrate or integrate these systems should be sufficient for control-testing purposes.				1. Interview responsible and/or accountable individuals to determine what methods the enterprise uses to transfer, integrate or incorporate on premises systems and AWS applications or related resources. 2. Obtain and inspect migration or data-transfer policies, procedures and/or processes to determine whether personnel are provided guidance and security requirements dictating network interactions between on premises systems communicating with AWS.				

Amazon Web Services® (AWS®) Audit Program
Governance

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Work paper	Pass/ Fail	Comments
Understanding Structure, Roles and Responsibilities		Use of AWS® services is strictly for business purposes and advances the enterprise's mission and strategic objectives.	The enterprise has a formal and independent governance structure (an AWS steering committee) that exists to guide initial development and ongoing operations of the AWS program. Note: This group should be separate from the enterprise personnel performing daily or routine operations that utilize AWS services and applications. This group should also be responsible for consulting with the board of directors to establish objective compliance criteria, approval and understanding of all AWS applications in use (e.g., S3, EC2, Amazon Cognito®, etc.), methods to measure compliance and reporting structures among themselves, the board of directors and operational personnel who are accountable to this group.				1. Interview responsible and/or accountable individuals who oversee AWS services within the enterprise (Chief Operating Officer, Chief Security Officer, etc.) and determine if a formal governance structure exists to drive development and usage of AWS services 2. Obtain and inspect documented enterprise organizational charts to determine if reporting and communication channels have been established between the board of directors, the governing body and personnel responsible for operating the AWS program 3. Obtain and inspect AWS program charters or related documentation outlining: a) Intended business purpose AWS services should achieve b) Compliance criteria and/or platform requirements c) Mechanisms used to measure program compliance or success (annual platform reviews, baselines/alerts, etc.) d) Routine review of the program charter occurs between board of directors and the governance structure to ensure AWS services continue to meet business needs				
		Alignment of AWS operations with AWS program requirements per the AWS steering committee is ensured through timely and ongoing clarity in roles and responsibilities.	On a regular basis (defined by the enterprise), the AWS steering committee meets with operational management personnel to discuss AWS program status. Note: These meetings should focus on the: • Governance structure providing feedback to operational management • Formal communication of staffing and resource needs required to operate the platform in accordance with stakeholder needs • Challenges which operational management faces with security or program implementation • Compliance concerns (or other matters) that may generally impact achievement of stakeholder needs				Obtain and inspect calendar invites, meeting minutes and/or summary AWS program status reports to determine if the governance structure is regularly communicating with personnel who perform daily AWS program operations.				
		Complete accountability is established over individual AWS applications and their related resources to ensure that the enterprise can meet stakeholders' expectations through a secure environment.	The enterprise has designated application owners responsible for accurately configuring AWS applications, assessing related risk and performing maintenance of AWS applications and related resources as necessary. Note: AWS has dozens of individual application and service offerings with AWS application owners taking on custodial roles. AWS application owners may be a single individual or a department, or may span several departments or individuals across the enterprise. AWS applications (e.g., S3, EC2®, IAM, etc.) are subject to code changes (or changes in general) under the control of AWS. New services also emerge constantly that may integrate with existing services. It is important that the entire suite of AWS applications and their related resources (S3 buckets, EC2 instances, and IAM users or roles) are owned, and that their capabilities are fully understood, assessed and strictly maintained in accordance with enterprise requirements.				1. If not already available in security program documentation, interview responsible and/or accountable individuals to understand the entire collection of AWS applications in use and the corresponding individual(s) or department(s) who manage each application. 2. Further inquire with these individuals to understand how each service, related resources and configuration methodologies are used to meet documented security or business requirements. Further determine requirements for documenting, communicating and resolving noncompliant services. 3. Obtain and inspect documentation describing intended business use of each service, completed risk assessments and/or completed reviews performed by individual AWS application owners documenting AWS application compliance and resolution (if necessary).				
		The enterprise's information security program and related procedures (inclusive of AWS services) remain current and relevant in light of operational changes.	The enterprise has developed formal security documentation (e.g., plans, policies and procedures) which incorporates the use of AWS services. Management performs an annual review of AWS security documentation in order to align documentation with operational changes to ensure completeness and accuracy.				1. Interview responsible and/or accountable individuals who maintain information security program plans or related documentation (e.g., chief security officer, etc.), to determine whether ongoing consideration is given to assessing, understanding, documenting and communicating security requirements for all AWS applications in use. 2. Obtain and inspect security-program documentation (e.g., security plan, policies, procedures, etc.), and determine whether existing documentation adequately describes: • AWS security requirements and how they are generally achieved • Instructions to personnel, detailing how to configure and maintain a compliant environment in accordance with documented requirements 3. Further inspect the related documents and determine whether: • An owner is documented for each directive that exists • Documents are formally reviewed by management, at least annually, for completeness and accuracy				

Amazon Web Services® (AWS®) Audit Program Governance											
Process Sub-area	*Ref. Risk*	*Control Objectives*	*Controls*	*Control Type*	*Control Classification*	*Control Frequency*	*Testing Step*	*Ref. Framework/ Standards*	*Ref. Work paper*	*Pass/ Fail*	*Comments*
Establishing AWS Directives		The enterprise has developed formal plans or policies and procedures for business critical AWS functions (including, but not limited to, change management and incident response).	The enterprise has developed formal change management, incident response and disaster recovery plans for AWS applications.				Interview individuals responsible and/or accountable for each policy/procedure that includes AWS services. Determine the frequency of plan (policy/procedure) review to ensure completeness/accuracy. Also, determine appropriateness of the following elements for each plan. a) Change management 1) Categories of changes (priority 1, 2, 3, emergency, etc.) 2) Required approvals per category 3) Documentation and retention period of change records 4) Approved change windows per change category 5) Testing requirements and back-out plans b) Security incident response 1) Phases of and responsibilities during an incident (discovery, investigation, communication, containment, eradication, recovery, etc.) 2) Crisis communication procedures 3) Call trees for necessary staff 4) Reporting requirements 5) Evidence collection, retention and postincident process for lessons learned and/or external reporting c) Disaster recovery 1) Identify completed business impact analysis (BIA) 2) Identify control measures to reduce risk (preventive, detective, corrective measures the enterprise will take) 3) Identify recovery strategies for critical enterprise and AWS applications 4) Identify recovery time objectives (RTO) per AWS application or related critical assets 5) Identify recovery point objectives (RPO) per AWS application or related critical assets 6) Identify documented recovery exercises to ensure the plan will work as intended along with plan maintenance				
Defining and Understanding Network Boundaries		The enterprise provides consistent levels of IT operational service through adequate network management, inclusive of AWS applications.	Management has documented network diagrams detailing all utilized AWS applications, data pathways and data participants. Diagrams are reviewed annually and updated as necessary. Note: Much like the human body and its various systems (musculoskeletal, central nervous system, etc.), appropriate network diagrams usually entail a series of layered diagrams that explain abstract—but related—concepts about the structure and flow of a given environment. In the case of AWS, it is important to understand the: • Number of root accounts in use • Number of virtual private clouds (VPCs) per root account • Regions each VPC has been deployed to (e.g., Northern Virginia; Frankfurt, Germany; etc.) • Peering connections between each VPC (if any) • Number of subnets per VPC • Configured gateways per VPC • Data riding along each connection				1. Interview responsible and/or accountable individuals (network architects or engineers) and determine the degree to which the overall AWS environment has been documented, with express attention to: a) Number of root accounts the enterprise has in use and is paying Amazon for (confirm using detailed billing statement(s); each root account has an individual account number, e.g., 4356789101) b) Number of virtual private clouds (VPCs) and the classless inter-domain routing (CIDR) notation of each VPC under each root account (each VPC will have a unique VPC-ID, if truly unique; CIDR will indicate how many subnets / networked hosts may exist within each VPC) c) VPC peering connections that exist (peering connections allow inter-VPC connectivity from the same or different AWS root accounts) d) individual AWS applications deployed to each individual VPC e) placement and general configuration of Internet, customer or NAT gateways receiving internet or external network traffic f) Business entities (parent enterprise, partner enterprises, extranets, etc.) that create, use or extract data (and the types of data traversing the network) 2. Further inquire into the frequency of reviews for appropriateness of items above, and what criteria or methods are used to identify inappropriate network configurations, data flow, data types, in-use applications or network behavior. 3. Obtain and inspect network diagrams and/or related documentation, and determine whether items described above are depicted and adequately described in each diagram. If the items are described in a diagram, determine whether data types, network pathways that data travels on and data recipients or participants are also depicted.				
Establishing a Complete and Accurate Inventory		The enterprise manages security configuration weaknesses by maintaining a complete and accurate AWS inventory.	AWS Config has been deployed to collect, display and report to management all AWS applications and related resources in use. Note: AWS Config is capable of a 100-percent complete and accurate IT inventory for deployed AWS applications (S3, EC2, Redshift, etc.) and related resources (S3 buckets, EC2 instances, Redshift clusters). It is important to understand what exists before assets can be adequately protected and their benefits (relative to cost) are understood.				1. Interview responsible and/or accountable individuals (network infrastructure or security) to determine whether (and how) the IT Inventory is documented and maintained for completeness/accuracy. If using AWS Config: a) From AWS Management Console, click "AWS Config." The dashboard will populate with resources specific to the VPC and region. b) On the left-hand side of the screen, click " Settings." Under "Resource Types to Record," determine whether the following are selected: 1) Record All Resources Supported in This Region 2) Include Global Resources (e.g., AWS IAM resources) c) Determine whether a retention period is configured for changes made to AWS resources (If not, confirm that the default of 7 years is selected). d) Determine whether an Amazon S3 bucket has been specified to store configuration changes to IT Assets recorded by AWS Config. 1) Locate and inspect the security settings for the specified S3 bucket to ensure that appropriate access security and data encryption configurations have been applied. e) Determine whether an SNS Topic is configured along with a subscriber (i.e., an email address to appropriate personnel) that will be notified in the event IT assets configurations are changed f) Steps b) through e) should be repeated for each region where resources have been deployed (e.g., Ohio, Northern Virginia, Northern California, etc.)				

Amazon Web Services® (AWS®) Audit Program
Governance

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	Ref. Framework/ Standards	Ref. Work paper	Pass/ Fail	Comments
Classifying the IT Inventory		The enterprise designs and applies asset protection commensurate with data classification.	The enterprise has developed and maintains an AWS application-tagging strategy to aid in the identification, protection and data retention of IT assets (labels). The labels are applied to AWS assets to appropriately classify data and to ensure required protections. Note: AWS provides an ability to "tag" resources with custom labels. Tagging facilitates identification and grouping of assets by using common business terminology (such as "confidential, sensitive, public, etc.") or by department and business use. Tagging further aids the enterprise in knowing which resources should have encryption applied or when data retention or data purge mechanisms should be triggered. A single tagging strategy should be developed, approved and used throughout the enterprise, to reduce confusion and misapplication of security controls or data classification based on tags.				1. Interview responsible and/or accountable individuals (operations management, application development, etc.) to determine if an AWS asset-tagging or labeling strategy exists and is formally documented. 2. Obtain and inspect tagging strategy documentation to understand the AWS tagging or labeling hierarchy and how it applies to individual AWS applications. 3. Through haphazard or random sampling, determine if the AWS tagging or labeling has been applied to assets as defined by the tagging strategy using the AWS Management Console.				
Accountability for IT Asset Acquisitions		The enterprise purchases or acquires appropriate AWS services that support business goals and stakeholder needs.	Purchases of AWS applications must be explicitly reviewed and approved by the appropriate, enterprise-defined department or group, prior to use. The business need for individual AWS applications is reviewed for appropriateness on a periodic basis, as defined by the enterprise. Note: AWS develops and releases new applications on a continuous basis (e.g., AWS Snowball®, AWS Glacier, AWS Glue, etc.). It is important for the enterprise to control expenses and approve the use only of those applications which the enterprise needs. Additionally, in order to control wasteful spending, the use of each application and its related resources should be reviewed on a routine basis to retire applications or resources that no longer serve a business need.				1. Interview responsible and/or accountable individuals (operations management, application development, purchasing, etc.) to determine the application-acquisition process for new AWS applications that the enterprise uses. Further determine: a) Individuals required to review and approve purchases b) Method used to document and retain approvals c) Level of involvement from accounts payable and purchasing personnel (determine whether these departments must also review for appropriateness) d) Purchasing limits that may trigger additional review and approval (e.g., anything over US $2,500 requires CEO approval, etc.) e) Which AWS applications in use have been subjected to the documented process (processes may have been developed after the environment was built) f) Timing thresholds, frequency and methods used to review each AWS application for business-use validity. Note that business validity during the first year may be more challenging to determine. 2. Build a population of services subjected to the documented process from step e). 3. Using a judgmental selection of AWS applications, determine whether the documented acquisition process has been followed.				
Managing External Providers		Engagement of external service providers does not jeopardize security expectations that the enterprise has established.	External service providers who render in-scope services to the enterprise must agree to enterprise security requirements before access to AWS applications and sensitive data is allowed. These providers are also subject to routine security assessments. Note: Standard contract language, annual reviews of SOC reports or security questionnaires may satisfy this control.				1. Interview accountable and/or responsible individuals (vendor management office, legal, security, etc.), and obtain standard contract language used for external providers. 2.Obtain a list of service providers and determine if standard contract language and assessment occurred prior to entering into agreement with third-party service providers. 3. Confirm that the agreements selected for testing were fully executed prior to the external providers being granted access to AWS applications or related data.				
Protecting AWS Root Accounts		The enterprise's strategic objectives are not delayed or disrupted by adverse actions resulting from unauthorized access.	Interactions with Amazon Web Services® that involve enterprise accounts require authentication before information is provided or changed. AWS root accounts have security questions registered with AWS support to authenticate users requesting support. Note: This provides an additional layer of security that requires AWS support to challenge users who are attempting to obtain account information or change root-account passwords. The security questions and answers are NOT configured by default.				1. Interview responsible and/or accountable individuals (operations management, security, etc.) to determine which AWS roles can access the billing console to view or set the security questions, where answers may be stored, and which individuals know the answers. It may be ideal for 2-3 individuals to know the information and have access to update the information in the event one is unavailable. 2. Verify AWS Management Console settings: a) Navigate to the billing console for each root account in question: https://console.aws.amazon.com/billing/home?#/account/ b) Scroll down to the Configure Security Challenge Questions section. c) Either questions are populated or a message indicating "Security Questions Are Not Currently Enabled" will be presented, indicating the security feature is not enabled.* *Center for Internet Security®, *CIS Amazon Web Services Foundations,* CIS Benchmarks™, v1.2.0, 23 May 2018, *https://www.cisecurity.org/benchmark/amazon_web_services/*				