CSA Consensus Assessments Initiative Questionnaire (CAIQ)

Jan 2025

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

The CSA Consensus Assessments Initiative Questionnaire provides a set of questions the CSA anticipates a cloud consumer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions which can then be used for a wide range of uses, including cloud provider selection and security evaluation. AWS has completed this questionnaire with the answers below. The questionnaire has been completed using the current CSA CAIQ standard, v4.0.2 (06.07.2021 Update).

Introduction

The Cloud Security Alliance (CSA) is a “not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing.” For more information, see https://cloudsecurityalliance.org/about/.
A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission.

CSA Consensus Assessments Initiative Questionnaire

Question ID	Question	CSP CAIQ New Response (2024 Changed)	SSRM Control Ownership - New Response (2024 - Changed)	CSP Implementation Description (Optional/Recommended) - New Response (2024 - Changed)	CSC Responsibilities (Optional/Recommended) - New Response (2024)
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. Maintaining customer trust and confidence is of the utmost importance to AWS. AWS works to comply with applicable federal, state, and local laws, statutes, ordinances, and regulations concerning security, privacy and data protection of AWS services in order to minimize the risk of accidental or unauthorized access or disclosure of customer content.	
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. Internal and external audits are planned and performed according to a documented audit schedule to review the continued performance of AWS against standards-based criteria, like the ISO/IEC 27001 and to identify improvement opportunities. Compliance reports from these assessments are made available to customers, enabling them to evaluate AWS. You can access assessments in AWS Artifact: https://aws.amazon.com/artifact. The AWS Compliance reports identify the scope of AWS services and regions assessed, as well the assessor's attestation of compliance. Customers can perform vendor or supplier evaluations by leveraging these reports and certifications.	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	AWS internal and external audit and assurance uses risk-based plans and approach to conduct assessments at least annually. AWS Compliance program covers sections including but not limited to assessment methodology, security assessment and results, and non-conforming controls.	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	CSP-owned	AWS maintains Security, Governance, Risk and Compliance relationships with internal and external parties to verity, monitor legal, regulatory, and contractual requirements. Should a new security directive be issued, AWS has documented plans in place to implement that directive with designated timeframes.	

A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	CSP-owned	Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001, Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards.	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	In alignment with ISO 27001, AWS maintains a Risk Management program to mitigate and manage risk. AWS management has a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	In alignment with ISO 27001, AWS maintains a Risk Management program to mitigate and manage risk. AWS management has a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.	
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes	CSP-owned	AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. Maintaining customer trust and confidence is of the utmost importance to AWS. AWS works to comply with applicable federal, state, and local laws, statutes, ordinances, and regulations concerning security, privacy and data protection of AWS services in order to minimize the risk of accidental or unauthorized access or disclosure of customer content.	
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	

AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	AWS maintains a systematic approach, to planning and developing new services for the AWS environment, to ensure the quality and security requirements are met with each release. The design of new services or any significant changes to current services follow secure software development practices and are controlled through a project management system with multi-disciplinary participation. Prior to launch, each of the following requirements must be reviewed: • Security Risk Assessment • Threat modeling • Security design reviews • Secure code reviews • Security testing • Vulnerability/penetration testing	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSC-owned	See response to Question ID AIS-02.1	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSP-owned	See response to Question ID AIS-02.1	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSP-owned	See response to Question ID AIS-02.1	
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	Where appropriate, a continuous deployment methodology is conducted to ensure changes are automatically built, tested, and pushed to production, with the goal of eliminating as many manual steps as possible. Continuous deployment seeks to eliminate the manual nature of this process and automate each step, allowing service teams to standardize the process and increase the efficiency with which they deploy code. In continuous deployment, an entire release process is a "pipeline" containing "stages”.	
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	Where appropriate, a continuous deployment methodology is conducted to ensure changes are automatically built, tested, and pushed to production, with the goal of eliminating as many manual steps as possible. Continuous deployment seeks to eliminate the manual nature of this process and automate each step, allowing service teams to standardize the process and increase the efficiency with which they deploy code. In continuous deployment, an entire release process is a "pipeline" containing "stages”.	

AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	Automated code analysis tools are run as a part of the AWS Software Development Lifecycle, and all deployed software undergoes recurring penetration testing performed by carefully selected industry experts. Our security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations. Refer to Best Practices for Security, Identity, & Compliance for further details. Refer to the Best Practices for Security, Identity, & Compliance website for further details - https://aws.amazon.com/architecture/security-identity-compliance/.	
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	CSP-owned	Static code analysis tools are run as a part of the standard build process, and all deployed software undergoes recurring penetration testing performed by carefully selected industry experts. Our security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations. Refer to the Best Practices for Security, Identity, & Compliance website for further details - https://aws.amazon.com/architecture/security-identity-compliance/.	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes	CSP-owned	Automated code analysis tools are run as a part of the AWS Software Development Lifecycle, and all deployed software undergoes recurring penetration testing performed by carefully selected industry experts. Our security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations. Refer to the Best Practices for Security, Identity, & Compliance website for further details - https://aws.amazon.com/architecture/security-identity-compliance/.	
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	The AWS business continuity policy is designed to ensure minimum outage time and maximum effectiveness of the recovery and reconstitution efforts. which include • Activation and Notification, • Recovery, and • Reconstitution Phase AWS business continuity mechanisms are designed to ensure minimum outage time and maximum effectiveness of the recovery and reconstitution efforts. AWS resiliency encompasses the processes and procedures to identify, respond to, and recover from a major event or incident within our environment.	
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	Shared CSP and CSC	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on AWS and business continuity.	See Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond whitepaper which describes how Amazon Web Services (AWS) and our customers in the financial services industry achieve operational resilience using AWS services. Refer to the following whitepaper - https://docs.aws.amazon.com/whitepapers/latest/aws-operational-resilience/aws-operational-resilience.html

BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	Shared CSP and CSC	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on AWS and business continuity.	See Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond whitepaper which describes how Amazon Web Services (AWS) and our customers in the financial services industry achieve operational resilience using AWS services. Refer to the following whitepaper - https://docs.aws.amazon.com/whitepapers/latest/aws-operational-resilience/aws-operational-resilience.html
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	Shared CSP and CSC	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on AWS and business continuity.	See Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond whitepaper which describes how Amazon Web Services (AWS) and our customers in the financial services industry achieve operational resilience using AWS services. Refer to the following whitepaper - https://docs.aws.amazon.com/whitepapers/latest/aws-operational-resilience/aws-operational-resilience.html
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned	The AWS business continuity plan details the three-phased approach that AWS has developed to recover and reconstitute the AWS infrastructure: • Activation and Notification Phase • Recovery Phase • Reconstitution Phase This approach ensures that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and omissions.	
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	Information System Documentation is made available internally to AWS personnel through the use of Amazon's Intranet site. Refer to ISO 27001 Appendix A Domain 12.	
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	AWS Business Continuity Policies and Plans have been developed and tested at least annually in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on AWS and business continuity at least annually	

BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned	The AWS Business Continuity policy provides a complete discussion of AWS services, roles and responsibilities, and AWS processes for managing an outage from detection to deactivation. AWS Service teams create administrator documentation for their services and store the documents in internal AWS document repositories. Using these documents, teams provide initial training to new team members that covers their job duties, on-call responsibilities, service specific monitoring metrics and alarms, along with the intricacies of the service they are supporting. Once trained, service team members can assume on-call duties and be paged into an engagement as a resolver. In addition to the documentation stored in the repository, AWS also uses GameDay Exercises to train coordinators and Service Teams in their roles and responsibilities.	
BCR-08.1	Is cloud data periodically backed up?	Yes	Shared CSP and CSC	AWS maintains a retention policy applicable to AWS internal data and system components in order to continue operations of AWS business and services. Critical AWS system components, including audit evidence and logging records, are replicated across multiple Availability Zones and backups are maintained and monitored.	This control is part of the shared responsibility model. Customers retain control and ownership of their content. When customers store content in a specific region, it is not replicated outside that region. It is the customer's responsibility to replicate content across regions if business needs require that. Backup and retention policies are the responsibility of the customer. AWS offers best practice resources to customers including guidance and alignment to the Well Architected Framework. Snapshots are AWS objects to which IAM users, groups, and roles can be assigned permissions, so that only authorized users can access Amazon backups. AWS Backup allows customers to centrally manage and automate backups across AWS services. The service enables customers to centralize and automate data protection across AWS services.
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	Shared CSP and CSC	See response to Question ID BCR-08.1	
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	CSC-owned		AWS Backup allows customers to centrally manage and automate backups across AWS services. For additional details, refer to - https://aws.amazon.com/backup

BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	Shared CSP and CSC	The AWS business continuity policy is designed to ensure minimum outage time and maximum effectiveness of the recovery and reconstitution efforts. which include • Activation and Notification, • Recovery, and • Reconstitution Phase AWS business continuity mechanisms are designed to ensure minimum outage time and maximum effectiveness of the recovery and reconstitution efforts. AWS resiliency encompasses the processes and procedures to identify, respond to, and recover from a major event or incident within our environment AWS maintains a ubiquitous security control environment across its infrastructure. Each data center is built to physical, environmental, and security standards in an active-active configuration, employing an n+1 redundancy model to ensure system availability in the event of component failure. Components (N) have at least one independent backup component (+1), so the backup component is active in the operation even if other components are fully functional. In order to eliminate single points of failure, this model is applied throughout AWS, including network and data center implementation. Data centers are online and serving traffic; no data center is “cold.” In case of failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.	AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	AWS tests the business continuity at least annually to ensure effectiveness of the associated procedures and the organization readiness. Testing consists of gameday exercises that execute on activities that would be performed in an actual outage. AWS documents the results, including lessons learned and any corrective actions that were completed.	
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	Yes	CSP-owned		
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Yes	CSP-owned	AWS maintains a ubiquitous security control environment across its infrastructure. Each data center is built to physical, environmental, and security standards in an active-active configuration, employing an n+1 redundancy model to ensure system availability in the event of component failure. Components (N) have at least one independent backup component (+1), so the backup component is active in the operation even if other components are fully functional. In order to eliminate single points of failure, this model is applied throughout AWS, including network and data center implementation. Data centers are online and serving traffic; no data center is “cold.” In case of failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.	

CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes	CSP-owned	AWS applies a systematic approach to managing change to ensure that all changes to a production environment are reviewed, tested, and approved. The AWS Change Management approach requires that the following steps be complete before a change is deployed to the production environment: 1. Document and communicate the change via the appropriate AWS change management tool. 2. Plan implementation of the change and rollback procedures to minimize disruption. 3. Test the change in a logically segregated, non-production environment. 4. Complete a peer-review of the change with a focus on business impact and technical rigor. The review should include a code review. 5. Attain approval for the change by an authorized individual. Where appropriate, a continuous deployment methodology is conducted to ensure changes are automatically built, tested, and pushed to production, with the goal of eliminating as many manual steps as possible. Continuous deployment seeks to eliminate the manual nature of this process and automate each step, allowing service teams to standardize the process and increase the efficiency with which they deploy code. In continuous deployment, an entire release process is a "pipeline" containing "stages".	
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned	See response to Question ID CCC-01.1	
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	CSP-owned	See response to Question ID CCC-01.1	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSP-owned	Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy.	

CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	No	CSP-owned	AWS notifies customers of changes to the AWS service offering in accordance with the commitment set forth in the AWS Customer Agreement. AWS continuously evolves and improves our existing services, and frequently adds new services. Our services are controlled using APIs. If we change or discontinue any API used to make calls to the services, we will continue to offer the existing API for 12 months. Additionally, AWS maintains a public Service Health Dashboard to provide customers with the real-time operational status of our services at http://status.aws.amazon.com/.	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned	See response to Question ID CCC-01.1	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	AWS performs deployment validations and change reviews to detect unauthorized changes to its environment and tracks identified issues to resolution.	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	Management reviews exceptions to security policies to assess and mitigate risks. AWS Security maintains a documented procedure describing the policy exception workflow on an internal AWS website. Policy exceptions are tracked and maintained with the policy tool and exceptions are approved, rejected, or denied based on the procedures outlined within the procedure document.	
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	Yes	CSP-owned	See response to Question ID CCC-08.1	
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	CSP-owned	AWS applies a systematic approach to managing change to ensure changes to a production environment are reviewed, tested, and approved. The AWS Change Management approach requires that the following steps be complete before a change is deployed to the production environment: 1. Document and communicate the change via the appropriate AWS change management tool. 2. Plan implementation of the change and rollback procedures to minimize disruption. 3. Test the change in a logically segregated, non-production environment. 4. Complete a peer-review of the change with a focus on business impact and technical rigor. The review should include a code review. 5. Attain approval for the change by an authorized individual. Where appropriate, a continuous deployment methodology is conducted to ensure changes are automatically built, tested, and pushed to production, with the goal of eliminating as many manual steps as possible. Continuous deployment seeks to eliminate the manual nature of this process and automate each step, allowing service teams to standardize the process and increase the efficiency with which they deploy code. In continuous deployment, an entire release process is a "pipeline" containing "stages".	

CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys, AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications.	AWS customers are responsible for managing encryption keys within their AWS environments. Customers can leverage AWS services such as AWS KMS and CloudHSM to manage the lifecycle of their keys according to internal policy requirements. See following: AWS KMS https://aws.amazon.com/kms/ AWS CloudHSM https://aws.amazon.com/cloudhsm/
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSP-owned	See response to CEK-01.1	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	AWS allows customers to use their own encryption mechanisms (for storage and in-transit) for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	Shared CSP and CSC	AWS has implemented data handling and classification requirements. Customers retain complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.	AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.

CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	Shared CSP and CSC	See response to CEK-01.1	AWS customers are responsible for managing encryption keys within their AWS environments according to their internal policy requirements.
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes	Shared CSP and CSC	See response to CEK-01.1	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	CSP-owned	AWS has established an information security management program with designated roles and responsibilities that are appropriately aligned within the organization. AWS management reviews and evaluates the risks identified in the risk management program at least annually. The risk management program encompasses the following phases: Discovery – The discovery phase includes listing out risks (threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities. Research – The research phase considers the potential impact(s) of identified risks to the business and its likelihood of occurrence and includes an evaluation of internal control effectiveness. Evaluate – The evaluate phase includes ensuring controls, processes and other physical and virtual safeguards in place to prevent and detect identified and assessed risks. Resolve – The resolve phase results in risk reports provided to managers with the data they need to make effective business decisions and to comply with internal policies and applicable regulations. Monitor – The monitor phase includes performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed.	

CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	Yes	CSC-owned		AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Yes	CSP-owned	AWS has established a formal, periodic audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSP-owned	AWS has established a formal, periodic audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.	
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	Shared CSP and CSC	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS and ISO 27001.	AWS customers are responsible for managing encryption keys within their AWS environments according to their internal policy requirements.
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	Customers determine whether they want to leverage AWS KMS to store encryption keys in the cloud or use other mechanisms (on-prem HSM, other key management technologies) to store keys within their on-premises environments.

CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance

CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance

CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance
CEK-19.1	Are processes, procedures, and technical measures to use compromised keys to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and CSC	AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS and ISO 27001.	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS.

CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	Environments used for the delivery of the AWS services are managed by authorized personnel and are located in an AWS managed data centers. Media handling controls for the data centers are managed by AWS in alignment with the AWS Media Protection Policy. This policy includes procedures around access, marking, storage, transporting, and sanitation. Live media transported outside of data center secure zones is escorted by authorized personnel.	
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	CSP-owned	When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 (“Guidelines for Media Sanitization”) as part of the decommissioning process. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Yes	CSP-owned	AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers’ systems and content. Maintaining customer trust and confidence is of the utmost importance to AWS. AWS works to comply with applicable federal, state, and local laws, statutes, ordinances, and regulations concerning security, privacy and data protection of AWS services in order to minimize the risk of accidental or unauthorized access or disclosure of customer content.	

DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	CSP-owned	Environments used for the delivery of the AWS services are managed by authorized personnel and are located in an AWS managed data centers. Media handling controls for the data centers are managed by AWS in alignment with the AWS Media Protection Policy. This policy includes procedures around access, marking, storage, transporting, and sanitation. Live media transported outside of data center secure zones is escorted by authorized personnel.	
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	AWS engages with external certifying bodies and independent auditors to review and validate our compliance with compliance frameworks. AWS SOC reports provide additional details on the specific physical security control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	CSP-owned	Environments used for the delivery of the AWS services are managed by authorized personnel and are located in an AWS managed data centers. Media handling controls for the data centers are managed by AWS in alignment with the AWS Media Protection Policy. This policy includes procedures around access, marking, storage, transporting, and sanitation. Live media transported outside of data center secure zones is escorted by authorized personnel.	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	

DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	CSP-owned	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools.	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	CSP-owned	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools.	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	CSP-owned	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. The AWS SOC reports provide additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. For more information on the design, layout and operations of our data centers, please visit this site: AWS Data Center Overview	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	CSP-owned	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. The AWS SOC reports provide additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. For more information on the design, layout and operations of our data centers, please visit this site: AWS Data Center Overview	
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes	CSP-owned	AWS manages equipment identification in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	CSP-owned	Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy.	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	CSP-owned	Authentication logging aggregates sensitive logs from EC2 hosts and stores them on S3. The log integrity checker inspects logs to ensure they were uploaded to S3 unchanged by comparing them with local manifest files. Access and privileged command auditing logs record every automated and interactive login to the systems as well as every privileged command executed. External access to data stored in Amazon S3 is logged and the logs are retained for at least 90 days, including relevant access request information, such as the data accessor IP address, object, and operation.	

DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	CSP-owned	Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy.	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	CSP-owned	Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy.	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	CSP-owned	AWS equipment is protected from utility service outages in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provide additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities.	
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	CSP-owned	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11 and link below for Data center controls overview: https://aws.amazon.com/compliance/data-center/controls/	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	CSP-owned	AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provide additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities. Please refer to link below for Data center controls overview: https://aws.amazon.com/compliance/data-center/controls/	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	CSP-owned	The AWS Security Operations Center performs quarterly threat and vulnerability reviews of datacenters and colocation sites. These reviews are in addition to an initial environmental and geographic assessment of a site performed prior to building or leasing. The quarterly reviews are validated by third parties during our SOC, PCI, and ISO assessments.	

DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSP-owned	AWS has implemented data handling and classification requirements which provide specifications around: • Data encryption • Content in transit and during storage • Access • Retention • Physical controls • Mobile devices • Handling requirements AWS services are content agnostic, in that they offer the same high level of security to customers, regardless of the type of content being stored. We are vigilant about our customers' security and have implemented sophisticated technical and physical measures against unauthorized access. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.	
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	CSP-owned	When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 (“Guidelines for Media Sanitization”) as part of the decommissioning process. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
DSP-04.1	Is data classified according to type and sensitivity levels?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.

DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	AWS maintains a systematic approach, to planning and developing new services for the AWS environment, to ensure the quality and security requirements are met with each release. The design of new services or any significant changes to current services follow secure software development practices and are controlled through a project management system with multi-disciplinary participation. Prior to launch, each of the following requirements must be reviewed: • Security Risk Assessment • Threat modeling • Security design reviews • Secure code reviews • Security testing • Vulnerability/penetration testing	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.

DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	NA	CSC-owned		This is a customer responsibility. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	Shared CSP and CSC	AWS has established a formal Data Subject Access Request (DSAR) according to General Data Protection Regulation (GDPR). For this they have to call AWS and open a ticket by contacting a CS Team Manager, who will then work with Legal to open a ticket which includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.	AWS customers are responsible for the management of the data (including adhering to applicable laws and regulations) they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes			

DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes			
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	NA	CSP-owned	Customer data is not used for testing.	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	Shared CSP and CSC	AWS maintains a retention policy applicable to AWS internal data and system components in order to continue operations of AWS business and services. Critical AWS system components, including audit evidence and logging records, are replicated across multiple Availability Zones and backups are maintained and monitored.	AWS customers are responsible for the management of the data they place into AWS services, including retention, archiving, and deletion policies and practices.
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	NA	CSC-owned		Customers control their customer content. With AWS, customers: • Determine where their customer content will be stored, including the type of storage and geographic region of that storage. • Customers can replicate and back up their customer content in more than one region, and we will not move or replicate customer content outside of the customer's chosen region(s), except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users. • Choose the secured state of their customer content. We offer customers strong encryption for customer content in transit or at rest, and we provide customers with the option to manage their own encryption keys. • Manage access to their customer content and AWS services and resources through users, groups, permissions and credentials that customers control.

DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Yes	CSP-owned	We are vigilant about our customers' privacy. AWS policy prohibits the disclosure of customer content unless we're required to do so to comply with the law, or with a valid and binding order of a governmental or regulatory body. Unless we are prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing customer content so they can seek protection from disclosure. It's also important to point out that our customers can encrypt their customer content, and we provide customers with the option to manage their own encryption keys. We know transparency matters to our customers, so we regularly publish a report about the types and volume of information requests we receive here: https://aws.amazon.com/compliance/amazon-information-requests/.	
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes	Shared CSP and CSC	See response to Question ID DSP-18.1	
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	NA	CSC-owned		This is a customer responsibility. Customers manage access to their customer content and AWS services and resources. We provide an advanced set of access, encryption, and logging features to help you do this effectively (such as AWS CloudTrail). We do not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. Customers choose the region(s) in which their customer content will be stored. We will not move or replicate customer content outside of the customer's chosen region(s), except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users. Customers choose how their
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. Maintaining customer trust and confidence is of the utmost importance to AWS. AWS works to comply with applicable federal, state, and local laws, statutes, ordinances, and regulations concerning security, privacy and data protection of AWS services in order to minimize the risk of accidental or unauthorized access or disclosure of customer content.	

GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	CSP-owned	AWS has established an information security management program with designated roles and responsibilities that are appropriately aligned within the organization. AWS management reviews and evaluates the risks identified in the risk management program at least annually. The risk management program encompasses the following phases: Discovery – The discovery phase includes listing out risks (threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities. Research – The research phase considers the potential impact(s) of identified risks to the business and its likelihood of occurrence and includes an evaluation of internal control effectiveness. Evaluate – The evaluate phase includes ensuring controls, processes and other physical and virtual safeguards in place to prevent and detect identified and assessed risks. Resolve – The resolve phase results in risk reports provided to managers with the data they need to make effective business decisions and to comply with internal policies and applicable regulations. Monitor – The monitor phase includes performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed.	
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSP-owned	Management reviews exceptions to security policies to assess and mitigate risks. AWS Security maintains a documented procedure describing the policy exception workflow on an internal AWS website. Policy exceptions are tracked and maintained with the policy tool and exceptions are approved, rejected, or denied based on the procedures outlined within the procedure document.	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	AWS has established an information security management program with designated roles and responsibilities that are appropriately aligned within the organization. AWS management reviews and evaluates the risks identified in the risk management program at least annually. The risk management program encompasses the following phases: Discovery – The discovery phase includes listing out risks (threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities. Research – The research phase considers the potential impact(s) of identified risks to the business and its likelihood of occurrence and includes an evaluation of internal control effectiveness. Evaluate – The evaluate phase includes ensuring controls, processes and other physical and virtual safeguards in place to prevent and detect identified and assessed risks. Resolve – The resolve phase results in risk reports provided to managers with the data they need to make effective business decisions and to comply with internal policies and applicable regulations. Monitor – The monitor phase includes performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed.	

GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	See response to Question ID GRC-05.1	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	AWS documents, tracks, and monitors its legal, regulatory, and contractual agreements and obligations. In order to do so, AWS performs and maintains the following activities: 1) Identifies and evaluates applicable laws and regulations for each of the jurisdictions in which AWS operates 2) Documents and implements controls to help ensure its conformity with statutory, regulatory, and contractual requirements relevant to AWS 3) Categorizes the sensitivity of information according to the AWS information security policies to help protect from loss, destruction, falsification, unauthorized access and unauthorized release 4) Informs and continually trains personnel that must be made aware of information security policies to help protect sensitive AWS information 5) Monitors for nonconformities to the information security policies with a process in place to take corrective actions and enforce appropriate disciplinary action AWS maintains relationships with internal and external parties to monitor legal, regulatory, and contractual requirements. Should a new security directives be issued, AWS creates and documents plans to implement the directive within a designated timeframe. AWS provides customers with evidence of its compliance with applicable legal, regulatory, and contractual requirements through audit reports, attestations, certifications and other compliance enablers. Visit aws.amazon.com/artifact for information on how to review the AWS external attestation and assurance documentation.	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	CSP-owned	AWS personnel are part of special interest groups, including relevant external parties such as security groups. AWS personnel use these groups to improve their knowledge about security best practices and to stay up to date with relevant security information.	
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	In accordance with applicable law, AWS requires that employees undergo a background screening at hiring, commensurate with their position and level of access. The AWS SOC reports provide additional details regarding the controls in place for background verification.	

HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	Yes	CSP-owned	AWS conducts background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities. The AWS SOC reports provide additional details regarding the controls in place for background verification.	
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	AWS has implemented data handling and classification requirements that provide specifications around: • Data encryption • Content in transit and during storage • Access • Retention • Physical controls • Mobile devices • Data handling requirements Employees are required to review and sign-off on an employment contract, which acknowledges their responsibilities to overall Company standards and information security.	
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	AWS roles and responsibilities for maintaining safe and secure working environment are reviewed by independent external auditors during audits for our SOC, PCI DSS and ISO 27001 compliance.	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	

HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. All access from remote devices to the AWS corporate environment is managed via VPN and MFA. The AWS production network is separated from the corporate network by multiple layers of security documented in various control documents discussed in other sections of this response.	AWS customers are responsible for access management within their AWS environments.
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	Upon termination of employee or contracts, AWS assets in their possessions are retrieved on the date of termination. In case of immediate termination, the employee/contractor manager retrieves all AWS assets (e.g., Authentication tokens, keys, badges) and escorts them out of AWS facility.	
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	AWS Human Resources team defines internal management responsibilities to be followed for termination and role change of employees and vendors. AWS SOC reports provide additional details.	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	Personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Additionally, upon hire, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy.	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	In alignment with ISO 27001 standard, AWS employees complete periodic role-based training that includes AWS Security training and requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to SOC reports for additional details.	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	AWS implements formal, documented policies and procedures that provide guidance for operations and information security within the organization and the supporting AWS environments. Policies address purpose, scope, roles, responsibilities and management commitment. All policies are maintained in a centralized location that is accessible by employees.	

HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	Amazon Legal Counsel manages and periodically revises the Amazon NDA to reflect AWS business needs.	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSP-owned	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. AWS roles and responsibilities are reviewed by independent external auditors during audits for our SOC, PCI DSS and ISO 27001 compliance.	
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	See response to Question ID HRS-11.1	
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. AWS roles and responsibilities are reviewed by independent external auditors during audits for our SOC, PCI DSS and ISO 27001 compliance.	
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	CSP-owned	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. All access from remote devices to the AWS corporate environment is managed via VPN and MFA. The AWS production network is separated from the corporate network by multiple layers of security documented in various control documents discussed in other sections of this response. Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.	
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Yes	CSP-owned	AWS has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employee as well as electronic mail messages and the posting of information via the Amazon intranet. Refer to ISO 27001 standard, Annex A, domain 7 and 8. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	In alignment with ISO 27001, AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. Access control procedures are systematically enforced through proprietary tools. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	

IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	AWS internal Password Policies and guidelines outlines requirements of password strength and handling for passwords used to access internal systems. AWS Identity and Access Management (IAM) enables customers to securely control access to AWS services and resources for their users. Additional information about IAM can be found on website at https://aws.amazon.com/iam/. AWS SOC reports provide details on the specific control activities executed by AWS.	
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	Shared CSP and CSC	Amazon personnel with a business need to access the management plane are required to first use multi-factor authentication, distinct from their normal corporate Amazon credentials, to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked.	AWS customers are responsible for access management within their AWS environments.
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	Shared CSP and CSC	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. All access from remote devices to the AWS corporate environment is managed via VPN and MFA. The AWS production network is separated from the corporate network by multiple layers of security documented in various control documents discussed in other sections of this response.	Customers retain the ability to manage segregations of duties of their AWS resources. AWS best practices for Identity & Access Management can be found here: https://docs.aws.amazon.com/IAM/. Search for AWS best practices for Identity & Access Management.
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	CSP-owned	See response to Question ID IAM-04.1	
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSP-owned	In alignment with ISO 27001, AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. Access control procedures are systematically enforced through proprietary tools. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	

IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	CSP-owned	Access privilege reviews are triggered upon job and/or role transfers initiated from HR system. IT access privileges are reviewed on a quarterly basis by appropriate personnel on a regular cadence. IT access from AWS systems is terminated within 24 hours of termination or deactivation. AWS SOC reports provide further details on User access revocation. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	CSP-owned	Access privilege reviews are triggered upon job and/or role transfers initiated from HR system. IT access privileges are reviewed on a quarterly basis by appropriate personnel on a regular cadence. IT access from AWS systems is terminated within 24 hours of termination or deactivation. AWS SOC reports provide further details on User access revocation. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	CSP-owned	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. All access from remote devices to the AWS corporate environment is managed via VPN and MFA. The AWS production network is separated from the corporate network by multiple layers of security documented in various control documents discussed in other sections of this response. Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	CSP-owned	Amazon personnel with a business need to access the management plane are required to first use multi-factor authentication, distinct from their normal corporate Amazon credentials, to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked. Refer to SOC2 report for additional details.	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	CSP-owned	Access to AWS systems are allocated based on least privilege, approved by an authorized individual prior to access provisioning. Duties and areas of responsibility (for example, access request and approval, change management request and approval, change development, testing and deployment, etc.) are segregated across different individuals to reduce opportunities for an unauthorized or unintentional modification or misuse of AWS systems. Group or shared accounts are not permitted within the system boundary.	

IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	No			
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. AWS logging and monitoring processes are reviewed by independent third-party auditors for our continued compliance with SOC, PCI DSS and ISO 27001 compliance.	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. AWS logging and monitoring processes are reviewed by independent third-party auditors for our continued compliance with SOC, PCI DSS and ISO 27001 compliance.	
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	CSP-owned	AWS controls access to systems through authentication that requires a unique user ID and password. AWS systems do not allow actions to be performed on the information system without identification or authentication. User access privileges are restricted based on business need and job responsibilities. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. New user accounts are created to have minimal access. User access to AWS systems (for example, network, applications, tools, etc.) requires documented approval from the authorized personnel (for example, user's manager and/or system owner) and validation of the active user in the HR system. Refer to SOC2 report for additional details.	

IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	Shared CSP and CSC	Amazon personnel with a business need to access the management plane are required to first use multi-factor authentication, distinct from their normal corporate Amazon credentials, to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked. Refer to SOC2 report for additional details.	AWS customers are responsible for access management within their AWS environments.
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSP-owned	AWS Identity, Directory, and Access Services enable you to add multi-factor authentication (MFA) to your applications.	
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned	AWS Identity and Access Management (IAM) enables customers to securely control access to AWS services and resources for their users. Additional information about IAM can be found on website at https://aws.amazon.com/iam/ AWS SOC reports provide details on the specific control activities executed by AWS.	
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	Shared CSP and CSC	Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data and server instances are logically isolated from other customers by default. Privileged user access controls are reviewed by an independent auditor during the AWS SOC, ISO 27001 and PCI audits.	AWS Customers retain control and ownership of their data. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	CSP-owned	Details regarding AWS APIs can be found on the AWS website at: https://docs.aws.amazon.com/	
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSP-owned	Details regarding AWS interoperability of each service can be found on the AWS website at: https://docs.aws.amazon.com/	

IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSP-owned	Details regarding AWS interoperability of each service can be found on the AWS website at: https://docs.aws.amazon.com/	
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSP-owned	Details regarding AWS interoperability of each service can be found on the AWS website at: https://docs.aws.amazon.com/	
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	CSC-owned		Details regarding AWS interoperability of each service can be found on the AWS website at: https://docs.aws.amazon.com/
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	CSP-owned	AWS APIs and the AWS Management Console are available via TLS protected endpoints, which provide server authentication. Customers can use TLS for all of their interactions with AWS. AWS recommends that customers use secure protocols that offer authentication and confidentiality, such as TLS or IPsec, to reduce the risk of data tampering or loss. AWS enables customers to open a secure, encrypted session to AWS servers using HTTPS (Transport Layer Security [TLS]).	
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	Shared CSP and CSC	AWS customer agreements include data related provisions upon termination. Details regarding contract termination can be found in the example customer agreement, see Section 7. Term; Termination - https://aws.amazon.com/agreement/.	

IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	AWS implements formal, documented policies and procedures that provide guidance for operations and information security within the organization and the supporting AWS environments. Policies address purpose, scope, roles, responsibilities and management commitment. All policies are maintained in a centralized location that is accessible by employees.	
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	Shared CSP and CSC	AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly. In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.	AWS customers are responsible for information security requirements such as capacity management, access management, data protection, monitoring, change management, vulnerability management, scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications within their AWS environment according to their internal policy requirements.
IVS-03.1	Are communications between environments monitored?	Yes	Shared CSP and CSC	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.	AWS customers are responsible for information security requirements such as logging and monitoring, capacity management, access management, data protection, change management, vulnerability management, scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications within their AWS environment according to their internal policy requirements.
IVS-03.2	Are communications between environments encrypted?	Yes	Shared CSP and CSC	AWS maintains Cryptography Standards to protect information in-transit and at-rest.	Customers retain complete control of how they choose to classify their content, where it is stored, used and protected from disclosure. AWS APIs are available via TLS protected endpoints, which provide server authentication. Customers can use TLS for all of their interactions with AWS and within their multiple environment. AWS provides open encryption methodologies and enables customers to encrypt and authenticate all traffic, and to enforce the latest standards and ciphers.

IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	Shared CSP and CSC	AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed and any unnecessary ports or protocols in use are corrected.	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage their AWS environments and associated access. Customers maintain information related to their data and individual architecture.
IVS-03.4	Are network configurations reviewed at least annually?	Yes	Shared CSP and CSC	Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and ISO 27001.	AWS customers are responsible for configuration management within their AWS environments.
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	Shared CSP and CSC	AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed and any unnecessary ports or protocols in use are corrected. Customers maintain information related to their data and individual architecture.	AWS customers are responsible for network management within their AWS environments.
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	Shared CSP and CSC	Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and ISO 27001.	AWS customers are responsible for server and system management within their AWS environments.
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	The development, test and production environments emulate the production system environment and are used to properly assess and prepare for the impact of a change to the production system environment. In order to reduce the risks of unauthorized access or change to the production environment, the development, test and production environments are logically separated.	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	CSP-owned	Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customers maintain full control over who has access to their data. Services which provide virtualized operational environments to customers (i.e., EC2) ensure that customers are segregated from one another and prevent cross-tenant privilege escalation and information disclosure via hypervisors and instance isolation.	

IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSC-owned		AWS offers a wide variety of services and partner tools to help customer migrate data securely. AWS migration services such as AWS Database Migration Service and AWS Snowmobile are integrated with AWS KMS for encryption. Learn more about AWS cloud migration services at: https://aws.amazon.com/cloud-data-migration/
IVS-08.1	Are high-risk environments identified and documented?	Yes	Shared CSP and CSC	AWS network segmentation is aligned with the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements.
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	CSP-owned	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS and ISO 27001 compliance.	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	AWS implements formal, documented policies and procedures that provide guidance for operations and information security within the organization and the supporting AWS environments. Policies address purpose, scope, roles, responsibilities and management commitment. All policies are maintained in a centralized location that is accessible by employees.	
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned	In alignment with ISO 27001 standards, audit logs are appropriately restricted and monitored. AWS SOC reports provide details on the specific control activities executed by AWS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance.	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	Shared CSP and CSC	AWS maintains logging and monitoring policy and standards for security related events for applications and underlying infrastructure.	AWS customers are responsible for the applications within their AWS environment.
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	Shared CSP and CSC	AWS Security Metrics are monitored and analyzed in accordance with ISO 27001 standard. Refer to ISO 27001 Annex A, domain 16 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	AWS customers are responsible for incident management within their AWS environments.

LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	In alignment with ISO 27001 standards, audit logs are appropriately restricted and monitored. AWS SOC reports provide details on the specific control activities executed by AWS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance.	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSP-owned	AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis. Upon assessment and discovery of risk, Amazon disables accounts that display atypical usage matching the characteristics of bad actors. The AWS Security team extracts all log messages related to system access and provides reports to designated officials. Log analysis is performed to identify events based on defined risk management parameters.	
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSP-owned	See response to Question ID LOG-005.1	
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSP-owned	AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. AWS logging and monitoring processes are reviewed by independent third-party auditors for our continued compliance with SOC, PCI DSS and ISO 27001 compliance.	
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	

LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events.	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	In alignment with ISO 27001 standards, audit logs are appropriately restricted and monitored. AWS SOC reports provide details on the specific control activities executed by AWS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance.	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	Shared CSP and CSC	AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. AWS logging and monitoring processes are reviewed by independent third-party auditors for our continued compliance with SOC, PCI DSS and ISO 27001 compliance.	AWS customers are responsible for key management within their AWS environments.
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	Shared CSP and CSC	AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	Customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	CSP-owned	Access to data center is logged. Only authorized users are allowed into data centers. Visitors follow the visitor access process and their relevant details along with business purpose is logged in the data center access log system. The access log is retained for 90 days unless longer retention is legally required.	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	CSP-owned	In alignment with ISO 27001 standards, audit logs are appropriately restricted and monitored. AWS SOC reports provide details on the specific control activities executed by AWS. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance.	

LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSP-owned	AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis. Upon assessment and discovery of risk, Amazon disables accounts that display atypical usage matching the characteristics of bad actors. The AWS Security team extracts all log messages related to system access and provides reports to designated officials. Log analysis is performed to identify events based on defined risk management parameters.	
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance.	
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	See response to Question ID SEF-01.1	
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSP-owned	See response to Question ID SEF-01.2	
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	See response to Question ID SEF-01.1	

SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSP-owned	AWS incident response plans are tested on at least on an annual basis.	
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	AWS Security Metrics are monitored and analyzed in accordance with ISO 27001 standard. Refer to ISO 27001 Annex A, domain 16 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition, refer to Best Practices for Security, Identity, & Compliance site for additional details - https://aws.amazon.com/architecture/security-identity-compliance.	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	AWS employees are trained on how to recognize suspected security incidents and where to report them. When appropriate, incidents are reported to relevant authorities. AWS maintains the AWS security bulletin webpage, located at: https://aws.amazon.com/security/security-bulletins, to notify customers of security and privacy events affecting AWS services. Customers can subscribe to the Security Bulletin RSS Feed to keep abreast of security announcements on the Security Bulletin webpage. The customer support team maintains a Service Health Dashboard webpage, located at: http://status.aws.amazon.com/ to alert customers to any broadly impacting availability issues.	
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	AWS maintains the AWS security bulletin webpage, located at: https://aws.amazon.com/security/security-bulletins , to notify customers of security and privacy events affecting AWS services. Customers can subscribe to the Security Bulletin RSS Feed to keep abreast of security announcements on the Security Bulletin webpage. The customer support team maintains a Service Health Dashboard webpage, located at: http://status.aws.amazon.com/ to alert customers to any broadly impacting availability issues.	
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	AWS maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Security and Compliance is a shared responsibility between AWS and the customer. The shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Refer to shared responsibility model: https://aws.amazon.com/compliance/shared-responsibility-model/	

STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	Security and Compliance is a shared responsibility between AWS and the customer. AWS Information Security Management System policies that are in scope for SSRM are reviewed and updated annually and as necessary. The shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Refer to shared responsibility model: https://aws.amazon.com/compliance/shared-responsibility-model/	
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	CSP-owned	Security and Compliance is a shared responsibility between AWS and the customer. AWS Information Security Management System policies that are in scope for SSRM are reviewed and updated annually and as necessary. The shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Refer to shared responsibility model: https://aws.amazon.com/compliance/shared-responsibility-model/	
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	CSP-owned	Security and Compliance is a shared responsibility between AWS and the customer. AWS Information Security Management System policies that are in scope for SSRM are reviewed and updated annually and as necessary. The shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Refer to shared responsibility model: https://aws.amazon.com/compliance/shared-responsibility-model/	
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	CSP-owned	Security and Compliance is a shared responsibility between AWS and the customer. This varies by cloud services used, the shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Refer to shared responsibility model: https://aws.amazon.com/compliance/shared-responsibility-model/	
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	Security and Compliance is a shared responsibility between AWS and the customer. The shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Refer to shared responsibility model: https://aws.amazon.com/compliance/shared-responsibility-model/	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	AWS has established a formal, periodic audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned		
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	AWS periodically reviews policies, procedures, and standards to enable effective governance of third party risk management.	

STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Yes	Shared CSP and CSC	AWS service agreements includes multiple provisions and terms. For additional details, refer to following sample AWS Customer Agreement online - https://aws.amazon.com/agreement/	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	CSP-owned		
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	CSP-owned	AWS has established a formal, periodic audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.	
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	CSP-owned	AWS documents clear and comprehensive policies, procedures, and standards to enable effective governance of third-party risk management.	
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned		

STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	CSP-owned		
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes	CSP-owned	The AWS Security team notifies and coordinates with the appropriate Service Teams when conducting security-related activities within the system boundary. Activities include, vulnerability scanning, contingency testing, and incident response exercises. AWS performs external vulnerability assessments at least quarterly and identified issues are investigated and tracked to resolution. Additionally, AWS performs unannounced penetration tests by engaging independent third-parties to probe the defenses and device configuration settings within the system.	
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	AWS's program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC reports provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes	CSP-owned	See response to Question ID TVM-01.1	

TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	CSP-owned	AWS' program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC reports provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	CSP-owned	AWS implements open source software or custom code within its services. All open source software to include binary or machine-executable code from third-parties is reviewed and approved by the Open Source Group prior to implementation, and has source code that is publicly accessible. AWS service teams are prohibited from implementing code from third parties unless it has been approved through the open source review. All code developed by AWS is available for review by the applicable service team, as well as AWS Security. By its nature, open source code is available for review by the Open Source Group prior to granting authorization for use within Amazon.	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSP-owned	AWS Security regularly performs penetration testing. These engagements may include carefully selected industry experts and independent security firms. AWS does not share the results directly with customers. AWS third-party auditors review the results to verify frequency of penetration testing and remediation of findings.	
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	No	CSP-owned	AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools. External vulnerability assessments are conducted by an AWS approved third party vendor at least quarterly.	
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	CSP-owned	AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools.	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	The AWS Security team notifies and coordinates with the appropriate Service Teams when conducting security-related activities within the system boundary. Activities include, vulnerability scanning, contingency testing, and incident response exercises. AWS performs external vulnerability assessments at least quarterly and identified issues are investigated and tracked to resolution. Additionally, AWS performs unannounced penetration tests by engaging independent third-parties to probe the defenses and device configuration settings within the system.	

TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	Shared CSP and CSC	AWS tracks metrics for internal process measurements and improvements that align with our policies and standards.	AWS customers are responsible for vulnerability management within their AWS environments.
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	AWS implements formal, documented policies and procedures that provide guidance for operations and information security within the organization and the supporting AWS environments. Policies address purpose, scope, roles, responsibilities and management commitment. All policies are maintained in a centralized location that is accessible by employees.	
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by AWS leadership at least annually or as needed basis.	
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	Yes	CSP-owned	Amazon has established baseline infrastructure standards in alignment with industry best practices. All software installations are still monitored by AWS security, and mandatory security controls and software is always required. Users cannot continue to use their laptop or desktop if required software is not installed. Their device will be quarantined from network access until the non-conformance is resolved.	
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSP-owned	Amazon has established baseline infrastructure standards in alignment with industry best practices This includes endpoint compatibility with operating systems and applications.	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSP-owned	Amazon has established baseline infrastructure standards in alignment with industry best practices. This includes endpoint inventory management.	

UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes	CSP-owned	Note: AWS employees do not access, process, or change customer data in the course of providing our services. AWS has separate CORP and PROD environments which are separated from each other via physical and logical controls. Amazon has established baseline infrastructure standards in alignment with industry best practices. All software installations are still monitored by AWS security, and mandatory security controls and software is always required. Users cannot continue to use their laptop or desktop if required software is not installed. Their device will be quarantined from network access until the non-conformance is resolved.	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSP-owned	Amazon has established baseline infrastructure standards in alignment with industry best practices. These include automatic lockout after defined period of inactivity.	
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSP-owned	Amazon has established baseline infrastructure standards in alignment with industry best practices. All software installations are still monitored by AWS security, and mandatory security controls and software is always required. Users cannot continue to use their laptop or desktop if required software is not installed. Their device will be quarantined from network access until the non-conformance is resolved.	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	Shared CSP and CSC	Note: AWS employees do not access, process, or change customer data in the course of providing our services. AWS has separate CORP and PROD environments which are separated from each other via physical and logical controls. AWS uses several different cryptographic tools and services. AWS offers AWS Key Management Service (AWS KMS) for creation, management (rotation/revocation/archival), and control of cryptographic keys across applications and AWS services. Refer to AWS SOC reports for more details on KMS. Refer to Best Practices for Security, Identity, & Compliance website for additional details - available at https://aws.amazon.com/architecture/security-identity-compliance/	Customers are provided tools to encrypt data within AWS environment to add additional layers of security. The encrypted data can only be accessed by authorized personnel with access to encryption keys.
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned	AWS' program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC reports provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSP-owned	Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering, software firewalls, and malware detection.	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	NA		AWS employees do not access, process, or change customer data in the course of providing our services. AWS has separate CORP and PROD environments which are separated from each other via physical and logical controls. AWS customers are responsible for the management of the data they place into AWS services. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.	

UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	No	CSP-owned		
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Yes	CSP-owned	AWS scope for mobile devices are iOS and Android based mobile phones and tablets. AWS maintains a formal mobile device policy and associated procedures. Specifically, AWS mobile devices are only allowed access to AWS corporate fabric resources and cannot access AWS production fabric where customer content is stored. AWS production fabric is separated from the corporate fabric by boundary protection devices that control the flow of information between fabrics. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific information system services. Access control lists and rule sets are reviewed and approved, and are automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule-sets and access control lists are up-to-date. Consequently, mobile devices are not relevant to AWS customer content access.	
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Yes	CSP-owned		

End of Standard

Further Reading

For additional information, see the following sources:

- AWS Compliance Quick Reference Guide
- AWS Answers to Key Compliance Questions
- AWS Cloud Security Alliance (CSA) Overview

Document Revisions

Date	Description
January 2025	Reviewed and updated responses to individual questions
November 2023	Reviewed and updated responses to individual questions
April 2022	Updated CAIQ template and updated responses to individual questions based on CAIQ v4.0.2
July 2018	2018 validation and update
January 2018	Migrated to new template.
January 2016	First publication