CSA Consensus Assessments Initiative Questionnaire (CAIQ)

February 2020

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, v3.1.1 (11-15-19 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	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AIS-01.1	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			The AWS system development lifecycle incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			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 AWS Overview of Security Processes for further details. That whitepaper is located here. https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf	AWS
AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?		X		Manual source-code analysis is not employed. Automated code analysis tools are run as a part of the AWS Software Development Lifecycle.	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			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 AWS Overview of Security Processes for further details. That whitepaper is located here. https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf Customers are responsible for performing vulnerability scanning of their workloads based on their internal scanning requirements.	Shared
AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			AWS and customers agree to a service agreement outlining the terms of service and responsibilities of both parties prior to service delivery.	Shared

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	X			AWS and customers agree to a service agreement outlining the terms of service and responsibilities of both parties prior to service delivery.	Shared
AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?	X			AWS data integrity controls as described in AWS SOC reports for S3, illustrates the data integrity controls maintained through all phases including transmission, storage and processing. Customers are responsible for control implementation related to Application interfaces and databases utilized within AWS environment.	Shared
AIS-03.2	Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			AWS data integrity controls as described in AWS SOC reports for S3, illustrates the data integrity controls maintained through all phases including transmission, storage and processing. Customers are responsible for control implementation related to Application interfaces and databases utilized within AWS environment.	Shared

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			AWS has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems and content. AWS maintains a broad range of industry and geography specific compliance programs and is continually assessed by external certifying bodies and independent auditors to provide assurance the policies, processes, and controls established and operated by AWS are in alignment with these program standards and the highest industry standards. Refer to: https://aws.amazon.com/compliance/programs/	AWS
AAC-01.1	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AAC-01.2	Does your audit program take into account effectiveness of implementation of security operations?	X			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.	AWS
AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			AWS provides third-party attestations, certifications, Service Organization Controls (SOC) reports and other relevant compliance reports directly to our customers under NDA.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			Although AWS Security regularly engages carefully selected industry experts and independent security firms to perform recurring penetration testing, we do not share the results directly with customers. Instead, the results are reviewed and validated by our auditors. Customers can request permission to conduct penetration testing to or originating from any AWS resources as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Penetration tests should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans. Advance approval for these types of scans can be initiated by submitting a request using the AWS Vulnerability / Penetration Testing Request Form found here: https://aws.amazon.com/security/penetration-testing/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			Although AWS Security regularly engages carefully selected industry experts and independent security firms to perform recurring penetration testing, we do not share the results directly with customers. Instead, the results are reviewed and validated by our auditors. Customers can request permission to conduct penetration testing to or originating from any AWS resources as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Penetration tests should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans. Advance approval for these types of scans can be initiated by submitting a request using the AWS Vulnerability / Penetration Testing Request Form found here: https://aws.amazon.com/security/penetration-testing/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AAC-02.4	Do you conduct internal audits at least annually?	X			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 audits are performed at a regular basis to cover different AWS products and services using a standards-based approach. Internal audit function operates independently of AWS teams and establishes a risk based approach to reviewing compliance to standards at AWS.	AWS
AAC-02.5	Do you conduct independent audits at least annually?	X			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.	AWS
AAC-02.6	Are the results of the penetration tests available to tenants at their request?		X		Although AWS Security regularly engages carefully selected industry experts and independent security firms to perform recurring penetration testing, we do not share the results directly with customers. Instead, the results are reviewed and validated by our auditors.	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
AAC-02.7	Are the results of internal and external audits available to tenants at their request?	X			AWS provides third-party attestations, certifications, Service Organization Controls (SOC) reports and other relevant compliance reports directly to our customers under NDA. AWS shares the results of internal audit with our external auditors but not directly with customers.	AWS
AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			AWS maintains relationships with internal and external parties to 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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-01.1	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			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.	AWS
BCR-01.2	Do you have more than one provider for each service you depend on?	X			Components (N) have at least one independent backup component (+1), so the backup component is active in the operation even if all 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. All 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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-01.3	Do you provide a disaster recovery capability?	X			AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. AWS SOC reports provide further details. ISO 27001 standard Annex A, domain 15 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-01.4	Do you monitor service continuity with upstream providers in the event of provider failure?	X			AWS maintains a ubiquitous security control environment across all regions. 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 all 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. All 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
BCR-01.5	Do you provide access to operational redundancy reports, including the services you rely on?		X		The information is shared with independent third party auditors and the results of those audit engagements are shared with customers.	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-01.6	Do you provide a tenant-triggered failover option?	X			AWS provides publicly available mechanisms for customers to report security and/or privacy events, including disasters.	Customer
BCR-01.7	Do you share your business continuity and redundancy plans with your tenants?		X		The information is shared with independent third-party auditors and the results of those audit engagements are shared with customers.	N/A
BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-03.1	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	X			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/	AWS
BCR-03.2	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	X			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/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			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.	AWS
BCR-05.1	Is physical damage anticipated and are countermeasures included in the design of physical protections?	X			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 or AWS SOC2 report and link below for Data center controls overview: https://aws.amazon.com/compliance/data-center/controls/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		X		Each AWS data center is evaluated to determine the controls that must be implemented to mitigate, prepare, monitor, and respond to natural disasters or malicious acts that may occur. 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/	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-07.1	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	X			AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. In order to ensure maintenance procedures are properly executed, AWS assets are assigned an owner, tracked and monitored with AWS proprietary inventory management tools. AWS asset owner procedures are carried out by method of utilizing a proprietary tool with specified checks that must be completed according to the documented maintenance schedule. Third party auditors test AWS equipment maintenance controls by validating that the asset owner is documented and that the condition of the assets are visually inspected according to the documented maintenance policy.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-07.2	Do you have an equipment and datacenter maintenance routine or plan?	X			AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. In order to ensure maintenance procedures are properly executed, AWS assets are assigned an owner, tracked and monitored with AWS proprietary inventory management tools. AWS asset owner procedures are carried out by method of utilizing a proprietary tool with specified checks that must be completed according to the documented maintenance schedule. Third party auditors test AWS equipment maintenance controls by validating that the asset owner is documented and that the condition of the assets are visually inspected according to the documented maintenance policy.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	X			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.	AWS
BCR-09.1	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			Policies and Procedures for continued service operations have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/compliance/programs	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-09.2	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X			Business Impact Assessment is performed to assign business criticality to supporting processes and identification of operational processes, teams and dependencies to sustain operations during a business disruption.	AWS
BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	X			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. Customers retain control and ownership of their content. 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 applicable retention policies. AWS customers can achieve data retention by leveraging whitepaper on AWS Well-Architected Framework available at: https://aws.amazon.com/security/security-learning/	Shared

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-11.2	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	X			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. Customers retain control and ownership of their content. 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 applicable retention policies. AWS customers can achieve data retention by leveraging whitepaper on AWS Well-Architected Framework available at: https://aws.amazon.com/security/security-learning/	Shared

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			Customers retain control and ownership of their content. 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 backup their content within AWS environment, to on-premises environment or backup tapes. AWS customers can achieve data backups by leveraging whitepaper on AWS Well-Architected Framework available at: https://aws.amazon.com/security/security-learning/	Customer
BCR-11.4	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			Customers can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair. More details are available at: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html EBS Snapshot functionality allows customers to capture and restore virtual machine images at any time.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	X			Customers can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair. More details are available at: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html EBS Snapshot functionality allows customers to capture and restore virtual machine images at any time.	Customer
BCR-11.6	Does your cloud solution include software/provider independent restore and recovery capabilities?	X			Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions).	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?			X	Customers retain control and ownership of their content. 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 backup their content within AWS environment, to on-premises environment or backup tapes. AWS customers can achieve data backups by leveraging whitepaper on AWS Well-Architected Framework available at: https://aws.amazon.com/security/security-learning/	Customer
CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			The design of all 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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
CCC-02.1	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	X			AWS applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on Amazon guidelines and tailored to the specifics of each AWS service. Refer to AWS SOC 2 report for additional information on AWS change management mechanisms.	AWS
CCC-02.2	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	X			AWS applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on Amazon guidelines and tailored to the specifics of each AWS service. Refer to AWS SOC 2 report for additional information on AWS change management mechanisms.	AWS
CCC-03.1	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			AWS maintains an ISO 9001 certification. This is an independent validation of AWS quality system and determined that AWS activities comply with ISO 9001 requirements.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
CCC-03.2	Is documentation describing known issues with certain products/services available?	X			AWS Security Bulletins notify customers of security and privacy events. Customers can subscribe to the AWS Security Bulletin RSS feed on our website. Refer to https://aws.amazon.com/security/security-bulletins/ AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to AWS Service Health Dashboard.	AWS
CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
CCC-03.4	Do you have controls in place to ensure that standards of quality are being met for all software development?	X			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. AWS' strategy for the design and development of services is to clearly define services in terms of customer use cases, service performance, marketing and distribution requirements, production and testing, and legal and regulatory requirements. The design of all 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. Requirements and service specifications are established during service development, taking into account legal and regulatory requirements, customer contractual commitments, and requirements to meet the confidentiality, integrity and availability of the service. Service reviews are completed as part of the development process.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
CCC-03.5	Do you have controls in place to detect source code security defects for any outsourced software development activities?			X	AWS does not outsource the development of AWS Services.	N/A
CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			The AWS system development lifecycle (SDLC) incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Refer to the AWS Overview of Security Processes whitepaper for further details. That whitepaper is located here. https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf	AWS
CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			General users do not have rights to install software to production environments. Before being installed to production environments, all software goes through the standard change management process enforced by AWS, including appropriate approvals.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		X		AWS does not provide this level of granularity to customers. 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.	N/A

CCC-05.2	Do you have policies and procedures established for managing risks with respect to change management in production environments?	X			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	AWS

					continuous deployment, an entire release process is a "pipeline" containing "stages”.	

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
CCC-05.3	Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	X			AWS developers that require access to production environments must explicitly request access through the AWS access management system, have the access reviewed and approved by the appropriate owner, and upon approval obtain authentication. AWS service teams maintain service specific change management standards that inherit and build on the AWS Change Management guidelines.	AWS
DSI-01.1	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	X			AWS provides the ability to tag EC2 resources. A form of metadata, EC2 tags can be used to create user- friendly names, enhance searchability, and improve coordination between multiple users. The AWS Management Console also supports tagging. AWS does not provide hardware to customers but virtual machines are assigned to customers as part of the EC2 service.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DSI-01.2	Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?		X		AWS does not provide hardware to customers but virtual machines are assigned to customers as part of the EC2 service.	N/A
DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?			X	AWS provides the required documentation and associated data flow diagrams for AWS services Customers determine the design patterns based on their usage of AWS services and associated network and system components.	Customer
DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	X			AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			AWS APIs are available via TLS protected endpoints, which provide server authentication. Customers can use TLS for all of their interactions with AWS. AWS provides open encryption methodologies and enables customers to encrypt and authenticate all traffic, and to enforce the latest standards and ciphers.	AWS
DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			AWS APIs are available via TLS protected endpoints, which provide server authentication. Customers can use TLS for all of their interactions with AWS. AWS provides open encryption methodologies and enables customers to encrypt and authenticate all traffic, and to enforce the latest standards and ciphers.	Shared

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DSI-04.1	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?			X	AWS Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.	Customer
DSI-04.2	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?			X	AWS Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.	Customer
DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	AWS Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			AWS does not access, process, or change customer data in the course of providing our services without customer content. AWS customers maintain ownership of their data and AWS does not utilize customer data in testing of AWS services (production or non-productions).	AWS
DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?			X	AWS Customers retain control and ownership of their own data. Refer to the AWS Customer Agreement for additional information.	Customer
DSI-07.1	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	X			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 AWS: Overview of Security Processes Whitepaper for additional details - available at: http://aws.amazon.com/security/security-learning/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800-88 (“Guidelines for Media Sanitization”), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements. Encryption of sensitive data is generally a good security practice, and AWS provides the ability to encrypt EBS volumes and their snapshots with AES-256. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage. In order to be able to do this efficiently and with low latency, the EBS encryption feature is only available on EC2's more powerful instance types (e.g., M3, C3, R3, G2).	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DCS-01.1	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			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.	AWS
DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	X			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. 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	AWS
DCS-03.1	Do you have a capability to use system geographic location as an authentication factor?	X			AWS provides the capability of conditional user access based on IP address. Customers can add conditions to control how users can use AWS, such as time of day, their originating IP address, or whether they are using SSL.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DCS-03.2	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			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.	AWS
DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DCS-05.1	Can you provide tenants with your asset management policies and procedures?	X			AWS does not provide confidential AWS policies and procedures directly to the customers AWS engages with external certifying bodies and independent auditors to review and validate our compliance with policies. AWS SOC reports provide additional details on the specific asset management related policies and control activities executed by AWS.	AWS
DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			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. Refer to AWS: Overview of Security Processes Whitepaper for additional details - available at: http://aws.amazon.com/security/security-learning/ AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. In addition, AWS SOC 1 and SOC 2 reports provides further information.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DCS-07.1	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	X			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.	AWS
DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	X			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.	AWS
EKM-01.1	Do you have key management policies binding keys to identifiable owners?	X			AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions 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/). Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. 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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	X			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/).	AWS
EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	X			Customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/).	AWS
EKM-02.3	Do you maintain key management procedures?	X			Internally, 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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	X			Customers can leverage AWS Key Management Systems (KMS) to create and manage encryption keys lifecycle (refer to https://aws.amazon.com/kms/).	Customer
EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	X			AWS does not utilize any third party or open source framework to manage encryption keys. AWS utilizes proprietary KMS and CloudHSM for key management, leveraging industry best practices, including NIST validated FIPS 140-2 based hardware.	AWS
EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?			X	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 AWS: Overview of Security Processes Whitepaper for additional details - available at: http://aws.amazon.com/security/security-learning/	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?			X	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 AWS: Overview of Security Processes Whitepaper for additional details - available at: http://aws.amazon.com/security/security-learning/	Customer
EKM-03.3	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			Internally, 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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			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 AWS: Overview of Security Processes Whitepaper for additional details - available at: http://aws.amazon.com/security/security-learning/	Customer
EKM-04.3	Do you store encryption keys in the cloud?			X	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 environment.	Customer
EKM-04.4	Do you have separate key management and key usage duties?			X	Customers determine separation of duties with regards to key management and key usage responsibilities.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			AWS has established baseline infrastructure standards, including for network components. AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet. Firewall policies (configuration files) are automatically pushed to firewall devices every 24 hours.	AWS
GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet. Firewall policies (configuration files) are automatically pushed to firewall devices every 24 hours.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
GRM-02.1	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	X			In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition, AWS maintains an AWS ISO 27018 certification. Alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content. For more information refer to the AWS Compliance ISO 27018 FAQ http://aws.amazon.com/compliance/iso-27018-faqs/ . In addition, AWS Customers retain control and ownership of their data and can implement data residency, security and retention requirements based on legal and regulatory requirements.	Shared
GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	X			In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition, AWS maintains an AWS ISO 27018 certification. Alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content. For more information refer to the AWS Compliance ISO 27018 FAQ http://aws.amazon.com/compliance/iso-27018-faqs/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			The Control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies. Refer to AWS Risk & Compliance whitepaper for additional details - available at http://aws.amazon.com/compliance	AWS
GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			AWS provides our customers with our ISO 27001 certification. The ISO 27001 certification is specifically focused on the AWS ISMS and measures how AWS internal processes follow the ISO standard. Certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms they are operating in alignment with the ISO 27001 certification standard. For additional information refer to the AWS Compliance ISO 27001 FAQ website: https://aws.amazon.com/compliance/iso-27001-faqs/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	X			AWS security policies are reviewed and approved on an annual basis by Leadership.	AWS
GRM-05.1	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	X			AWS management leads an information security program that identifies and establishes security goals that are relevant to business requirements. Annual evaluations are performed to allocate the resources necessary for performing information security activities within AWS to meet or exceed customer and service specifications.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
GRM-06.2	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	X			AWS management leads an information security program that identifies and establishes security goals that are relevant to business requirements. Annual evaluations are performed to allocate the resources necessary for performing information security activities within AWS to meet or exceed customer and service specifications.	AWS

GRM-06.3	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			AWS creates and maintains written agreements with third parties (for example, Contractors or vendors) in accordance with the work or service to be provided (for example, network services agreement, service delivery agreement, or information exchange agreement) and implements appropriate relationship management mechanisms in line with their relationship to the business. Agreements cover, at a minimum, the following: • Legal and regulatory requirements applicable to AWS • User awareness of information security responsibilities and issues • Arrangements for reporting, notification, and investigation of information security incidents and security breaches • Target and unacceptable levels of service (for example, SLA, OLA) • Service continuity requirements (e.g., recovery time objectives - RTO), in accordance with AWS business priorities • Protection of Intellectual Property Rights (IPR) and copyright assignment of AWS • Conditions for renegotiation/termination of the agreement.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
GRM-06.4	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X			Information about the AWS Compliance programs is published publicly on our website at: http://aws.amazon.com/compliance/programs AWS provides multiple mappings to regulations and controls frameworks in public domain as well under NDA via AWS Artifact.	AWS
GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X			Information about the AWS Compliance programs is published publicly on our website at: http://aws.amazon.com/compliance/programs	AWS
GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			Employees who violate Amazon standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed.	AWS
GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			Employees who violate Amazon standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			Updates to AWS security policies, procedures, standards and controls occur as a result of periodic risk assessments or on an annual basis in alignment with the ISO 27001 standard Refer to ISO 27001 for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.	AWS
GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?		X		AWS information security and/or privacy policies are subject to change based on various inputs, including, risk assessment activities, regulatory or legal guidance, follow-up to audit reviews etc. We do not provide policy details to our tenants, but these are validated and certified by independent auditors that confirm our compliance with ISO 27001, SOC2 and PCI DSS. Any changes to AWS published controls will be available to customers as part of published compliance reports and audit documents.	N/A
GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	X			AWS security policies are reviewed and approved on an annual basis by Leadership.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			In alignment with ISO 27001 AWS has developed a Risk Management program to mitigate and manage risk. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. Refer to AWS Risk and Compliance Whitepaper (available at http://aws.amazon.com/security/security-learning/) for additional details on AWS Risk Management Framework.	AWS
GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X			In alignment with ISO 27001 AWS has developed a Risk Management program to mitigate and manage risk. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. Refer to AWS Risk and Compliance Whitepaper (available at http://aws.amazon.com/security/security-learning/) for additional details on AWS Risk Management Framework.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	X			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.	AWS
GRM-11.2	Do you make available documentation of your organization-wide risk management program?		X		AWS Risk Management program is reviewed by independent external auditors during audits for our PCI DSS and ISO 27001 compliance. .	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			Upon termination, Human Resources ensures that a formal checklist, which includes steps for access removal and collection of assets, is completed by HR or the terminated employee's manager. AWS is responsible for the following processes upon the termination of an employee or contractors: • Communicating termination responsibilities, such as security requirements, legal responsibilities, and non-disclosure obligations to terminated personnel. • Revoking information system access. • Retrieving all AWS information system-related property (e.g. authentication tokens, keys, badges). • Disabling badge access (automated).	AWS
HRS-01.2	Do you have asset return procedures outlining how assets should be returned within an established period?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			AWS conducts criminal 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.	AWS
HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-03.2	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	X			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.	AWS
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provide further details on User access revocation. In addition, the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			Amazon Legal Counsel manages and periodically revises the Amazon NDA to reflect AWS business needs.	AWS
HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			The AWS Cloud Security Whitepaper and the AWS Risk and Compliance Whitepaper provide details on the roles and responsibilities of AWS and those of our Customers. The whitepapers area available at: http://aws.amazon.com/security/security-learning/ and http://aws.amazon.com/compliance/programs	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-08.1	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-08.2	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	X			AWS has a documented BYOD policy that outlines the procedures for employees to Bring their own device for use at Amazon. The users are required to comply with all Amazon policies. All devices are managed by AWS. All software installations are still monitored by AWS security, and mandatory security controls and software is always required.	AWS
HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-09.2	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			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.	AWS
HRS-09.3	Do you document employee acknowledgment of training they have completed?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-09.4	Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes. The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties.	AWS
HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	X			The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes. The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-09.6	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			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. In addition, the AWS: Overview of Security Processes Whitepaper provides further details - available at: http://aws.amazon.com/security/security-learning/	AWS
HRS-10.2	Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			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.	AWS
HRS-11.1	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			Amazon has established baseline infrastructure standards in alignment with industry best practices. These include automatic lockout after defined period of inactivity.	AWS
HRS-11.2	Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	X			AWS policies and procedures for maintaining safe and secure working environment are reviewed by independent external auditors during audits for our SOC, PCI DSS and ISO 27001 compliance.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			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.	AWS

IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			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, the AWS Security White paper, section "Employee Lifecycle" provides additional information. 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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-02.2	Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	X			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.	AWS
IAM-02.3	Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-02.4	Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-02.5	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-02.6	Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	X			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
IAM-02.7	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		X		AWS tracks metrics for internal process measurements and improvements, but this level of detail is not shared as it constitutes internal proprietary information.	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			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.	AWS
IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			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
IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			Customers retain the ability to manage segregations of duties of their AWS resources. AWS best practices for Identity & Access Management can be found here: AWS IAM Best Practices Internally, AWS aligns with ISO 27001 standards for managing segregation of duties. Refer to ISO 27001 standard, Annex A, domain 6 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard	Shared

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outline the controls in place to manage access provisioning to AWS resources. In addition, the AWS: Overview of Security Processes Whitepaper provides further details - available at: http://aws.amazon.com/security/security-learning/	AWS
IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outline the controls in place to manage access provisioning to AWS resources. In addition, the AWS: Overview of Security Processes Whitepaper provides further details - available at: http://aws.amazon.com/security/security-learning/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-07.1	Does your organization conduct third-party unauthorized access risk assessments?			X	AWS does not utilize third parties to provide services to customers, but does utilize co-location provides in limited capacity to house some AWS data centers. These controls are audited twice annually in our SOC 1/2 audits and annually in our ISO 27001/17/18 audits. There are no subcontractors authorized by AWS to access any customer-owned content that customers upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/	N/A
IAM-07.2	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropraite access?			X	AWS does not utilize third parties to provide services to customers, but does utilize co-location provides in limited capacity to house some AWS data centers. These controls are audited twice annually in our SOC 1/2 audits and annually in our ISO 27001/17/18 audits. There are no subcontractors authorized by AWS to access any customer-owned content that customers upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	X			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. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. 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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-08.2	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	X			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. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. 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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-08.3	Do you limit identities' replication only to users explicitly defined as business necessary?	X			Access to AWS systems are allocated based on least privilege, approved by an authorized individual prior to access provisioning, and assigned a different user ID than used for normal business use. 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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			Unique user identifiers are created as part of the onboarding workflow process in the AWS human resources management system. The device provisioning process helps ensure unique identifiers for devices. Both processes include manager approval to establish the user account or device. Initial authenticators are delivered to user's in-person and to devices as part of the provisioning process. Internal users can associate SSH public keys with their account. System account authenticators are provided to the requestor as part of the account creation process after the identity of the requestor is verified.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-09.2	Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X			AWS has established controls to address the threat of inappropriate insider access. All certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	X			In alignment with ISO 27001 standard, all access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked. Controls specific to User Access reviews are outlined in the SOC reports. Exceptions in the User entitlement controls are documented in the SOC reports.	AWS
IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			In alignment with ISO 27001 standard, all access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked. Controls specific to User Access reviews are outlined in the SOC reports. Exceptions in the User entitlement controls are documented in the SOC reports.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-10.3	Do you ensure that remediation actions for access violations follow user access policies?	X			In alignment with ISO 27001 standard, all access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked. Controls specific to User Access reviews are outlined in the SOC reports. Exceptions in the User entitlement controls are documented in the SOC reports.	AWS
IAM-10.4	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?			X	AWS Customers retain control and ownership of their data. 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.	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provide further details on User access revocation. In addition, the AWS Security White paper, section "Employee Lifecycle" provides additional information.	AWS
IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provide further details on User access revocation. In addition, the AWS Security White paper, section "Employee Lifecycle" provides additional information.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			The AWS Identity and Access Management (IAM) service provides identity federation to the AWS Management Console. Multi-factor authentication is an optional feature that a customer can utilize. Refer to the AWS website for additional details - http://aws.amazon.com/mfa AWS Identity and Access Management (IAM) supports identity federation for delegated access to the AWS Management Console or AWS APIs. With identity federation, external identities (federated users) are granted secure access to resources in your AWS account without having to create IAM users. These external identities can come from your corporate identity provider (such as Microsoft Active Directory or from the AWS Directory Service) or from a web identity provider, such as Amazon Cognito, Login with Amazon, Facebook, Google or any OpenID Connect (OIDC) compatible provider.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	X			With AWS Identity, Directory, and Access services, customers can easily add sign-up and sign-in functionality to their applications and create scalable cloud-native directories for your application users. Customers also can enable users to bring their own identities from social identity providers, such as Facebook and Amazon, or use their existing corporate identities through SAML. To help protect access to their application's user accounts, AWS Identity, Directory, and Access Services enable you to add multi-factor authentication (MFA) to your applications.	AWS
IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	X			AWS offers multiple options for federating your identities in the AWS Cloud. With federation, you can use single sign-on (SSO) to access your AWS accounts using credentials from your corporate directory. Federation uses open standards, such as Security Assertion Markup Language 2.0 (SAML), to exchange identity and security information between an identity provider (IdP) and an application. Learn more at: https://aws.amazon.com/identity/federation/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	X			Customers can enable Policy Enforcement capability using their existing Identity Providers and established fine grained policies to manage permissions to AWS resources.	Customer
IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	X			Using AWS Identity, Directory, and Access services, customers can manage user access to AWS accounts and business applications using their existing corporate identities and define fine-grained access policies to manage permissions to their AWS resources.	AWS
IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X			AWS Identity, Directory, and Access Services enable you to add multi-factor authentication (MFA) to your applications.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-12.7	Do you allow tenants to use third-party identity assurance services?	X			Customers can enable users to bring their own identities from social identity providers, such as Facebook and Amazon, or use their existing corporate identities through SAML.	AWS
IAM-12.8	Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	X			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.	AWS
IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	X			Customers can configure password policies and associated configurations for their accounts.	Customer
IAM-12.10	Do you support the ability to force password changes upon first logon?	X			Customers can configure password policies and associated configurations for their accounts.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X			Customers can configure password policies and associated configurations (e.g. account lockout etc.) for their accounts.	Customer

IAM-13.1	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	X			AWS has established and maintains company-wide policy that defines roles, responsibilities and classifications for managing changes to the production environment. Changes to AWS services and features follow secure software development practices, which include a security risk review prior to launch. AWS developers that require access to production environments must explicitly request access through the AWS access management system, have the access reviewed and approved by the appropriate owner, and upon approval obtain authentication. AWS service teams maintain service specific change management standards that inherit and build on the AWS Change Management guidelines. AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet. Firewall policies (configuration files) are automatically pushed to firewall devices every 24 hours. In order to validate that changes follow the standard change management procedures, all changes to the AWS production environment are reviewed on at least a monthly. An audit trail of the changes is maintained for a	AWS

					least a year. Emergency changes follow the AWS incident response procedures. Exceptions to the change management processes are documented and escalated to AWS management.	

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			AWS Security performs regular vulnerability scans on the underlying infrastructure, 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, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans.	Shared

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	X			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. Refer to AWS: Overview of Security Processes for additional details - available at: http://aws.amazon.com/security/security-learning/	AWS
IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	X			AWS provides multiple mappings to regulations and controls frameworks in public domain as well under NDA via AWS Artifact.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-01.4	Are audit logs centrally stored and retained?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			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.	AWS
IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?		X		Virtual Machines are assigned to customers as a part of the EC2 service. Customers retain control over what resources are being used and where resources reside. Refer to the AWS website for additional details - http://aws.amazon.com	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-02.2	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	X			AWS provides tools such as AWS Config to assess, audit and evaluate resource configurations. AWS Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. Customers are responsible for defining Config rulesets and necessary actions upon non-conformance. For more details see: https://aws.amazon.com/config/	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-02.3	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	X			Customers have the option to leverage available Amazon Machine Images (AMI) publicly available or utilize an approved internal image. AWS is designed to protect the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help ensure that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected. AWS enables customers to open a secure, encrypted session to AWS servers using HTTPS (Transport Layer Security [TLS]). Additionally, AWS offers customers the ability to add an additional layer of security to data at rest in the cloud, providing scalable and efficient encryption features. It is the responsibility of the AWS customer to enable these features for their system.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			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.	AWS
IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	X			Details regarding AWS Service Limits and how to request an increase for specific services is available on the AWS website at: https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html AWS manages capacity and utilization data 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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	X			AWS does not oversubscribe memory on the EC2 hypervisor. AWS offers multiple options to the customers to support their specific use cases. An EC2 Dedicated Host is a dedicated server of a specific Instance Class that is allotted to a single customer, referred to as dedicated tenancy. Dedicated hosts have a fixed number of vCPU and RAM per Instance Type. EC2 Instance Types offer multiple fixed vCPU to memory configurations to match the customer's workloads and use cases. EC2 Bare Metal instances and VMware Cloud on AWS gives the customer full control of the configuration of instances just as they have on-premise.	AWS
IVS-04.3	Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X			AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X			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
IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			The Amazon EC2 hypervisor is based on open source platforms. Independent auditors regularly assess the security of Amazon EC2 for new and existing vulnerabilities and internal and external penetration teams regularly search for attack vectors. As such, Amazon EC2 is well suited for maintaining strong isolation between guest virtual machines. 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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	X			AWS website provides guidance on creating a layered security architecture in a number of white papers available via the AWS public website: http://aws.amazon.com/documentation/	AWS
IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X			Several network fabrics exist at Amazon, each separated by devices that control the flow of information between fabrics. The flow of information between fabrics is established by approved authorizations, which exist as access control lists (ACL) which reside on these devices. These devices control the flow of information between fabrics as mandated by these ACLs. ACLs are defined, approved by appropriate personnel, managed and deployed using AWS ACL-manage tool. Customers maintain information related to their data flow and individual application architectures of their AWS implementations.	Shared

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X			Amazon's Information Security team approves these ACLs. 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. AWS Network Management is regularly reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, and ISO 27001 Customers maintain information related to their data and individual architecture.	Shared

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-06.4	Are all firewall access control lists documented with business justification?	X			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.	Shared
IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			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

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			AWS Customers retain the ability and the responsibility to create and maintain production and test environments. AWS website provides guidance on creating an environment utilizing the AWS services - http://aws.amazon.com/documentation/ AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with ISO 27001 standards. Refer to ISO 27001 standard, Annex A. domain 13 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	X			AWS Customers retain the ability and the responsibility to create and maintain production and test environments. AWS website provides guidance on creating an environment utilizing the AWS services - http://aws.amazon.com/documentation/ AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with ISO 27001 standards. Refer to ISO 27001 standard, Annex A. domain 13 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	Customer
IVS-08.3	Do you logically and physically segregate production and non-production environments?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			Internally, AWS network segmentation is aligned with ISO 27001 standards. Refer to ISO 27001 standard, Annex A. domain 13 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	AWS
IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X			Internally, AWS network segmentation is aligned with ISO 27001 standards. Refer to ISO 27001 standard, Annex A. domain 13 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-09.3	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	X			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. Different instances running on the same physical machine are isolated from each other via the hypervisor. In addition, the Amazon EC2 firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance’s neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical random-access memory (RAM) is separated using similar mechanisms.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-09.4	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			AWS gives customers ownership and control over their content by design through simple, but powerful tools that allow customers to determine where their content will be stored, how it will be secured in transit or at rest, and access to their AWS environment will managed. AWS has implemented global privacy and data protection best practices in order to helping customers establish, operate and leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.	Customer
IVS-09.5	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			AWS services are content agnostic, customers are responsible for designing workloads with adequate protections aligned to their control frameworks/standards.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			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/	Customer
IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?			X	AWS Customers retain control and ownership of their own data. AWS provides customers the ability to maintain and develop production and non-production environments. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization. Refer to AWS SOC reports for more information on Access Controls.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	Policies, procedures and mechanisms to protect AWS network environment are in place. There are no wireless networks or radio signals within the system boundary. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS and ISO 27001 compliance.	N/A
IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			X	There are no wireless networks or radio signals within the system boundary. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system.	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			X	There are no wireless networks or radio signals within the system boundary. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system.	N/A
IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?			X	AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, 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.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	X			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.	AWS
IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			Details regarding AWS APIs can be found on the AWS website at: https://aws.amazon.com/documentation/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			AWS customers can export data out of AWS environments in any industry supported format.	Customer
IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?			X	Customer retain control and ownership of their content. Customers can choose how they migrate applications and content both on and off the AWS platform at their discretion.	Customer
IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	X			Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions).	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IPY-03.3	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?		X		Customer retain control and ownership of their content. Customers can choose how they migrate applications and content both on and off the AWS platform at their discretion.	Customer
IPY-04.1	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			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]).	Customer
IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			Details regarding AWS interoperability of each service can be found on the AWS website at: https://aws.amazon.com/documentation/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interodperability?	X			The Amazon EC2 hypervisor is based on open source platforms. Independent auditors regularly assess the security of Amazon EC2 for new and existing vulnerabilities and internal and external penetration teams regularly search for attack vectors. As such, Amazon EC2 is well suited for maintaining strong isolation between guest virtual machines.	AWS
IPY-05.2	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	X			Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions).	Customer
IPY-05.3	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?		X		AWS uses customized Xen and/or KVM based hypervisor technology. AWS does not share internal proprietary information with customers, but the hypervisor configuration and management processes are reviewed as part of SOC2 and ISO assessments. Details can be obtained at: https://aws.amazon.com/ec2/nitro/	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			X	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.	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			X	See Response to MOS-01.1	N/A
MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			X	See Response to MOS-01.1	N/A
MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	See Response to MOS-01.1	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?			X	See Response to MOS-01.1	N/A
MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			X	See Response to MOS-01.1	N/A
MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			X	See Response to MOS-01.1	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			X	See Response to MOS-01.1	N/A
MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			X	See Response to MOS-01.1	N/A
MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			X	See Response to MOS-01.1	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			X	See Response to MOS-01.1	N/A
MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			X	See Response to MOS-01.1	N/A
MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			X	See Response to MOS-01.1	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X	See Response to MOS-01.1	N/A
MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?			X	See Response to MOS-01.1	N/A
MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X	See Response to MOS-01.1	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			X	See Response to MOS-01.1	N/A
MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			X	See Response to MOS-01.1	N/A
MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?			X	See Response to MOS-01.1	N/A
MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			X	See Response to MOS-01.1	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	See Response to MOS-01.1	N/A
MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X	See Response to MOS-01.1	N/A
MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X	See Response to MOS-01.1	N/A
MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	See Response to MOS-01.1	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			X	See Response to MOS-01.1	N/A
MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			X	See Response to MOS-01.1	N/A
MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			X	See Response to MOS-01.1	N/A
MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	See Response to MOS-01.1	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X	See Response to MOS-01.1	N/A
SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			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.	AWS
SEF-02.1	Do you have a documented security incident response plan?	X			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, the AWS: Overview of Security Processes Whitepaper provides further details - available at: http://aws.amazon.com/security/security-learning/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?		X		Customers are responsible for developing their incident response process based on their workloads and requirements.	Customer
SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	X			AWS offers customers a variety of support mechanism, including Enterprise Support to meet their internal incident response roles and responsibilities. For more detailed description of AWS incident management guidelines see: https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf	AWS
SEF-02.4	Have you tested your security incident response plans in the last year?	X			AWS incident response plans are tested on at least an annual basis.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X			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.	AWS

SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			AWS contingency plans and incident response playbooks have defined and tested tools and processes to detect, mitigate, investigate, and report a security incident. It includes guidelines for responding to and reporting a data breach in accordance with customer agreements. AWS security engineers follow a protocol when responding to a data security incident. The protocol involves steps which include validating customer data existence within the AWS service, determining the encryption status of a customer's content, and determining unauthorized access to a customer's content to the extent able. If any step in the event does not reveal a positive indicator, the security engineer documents the findings in internal tools used to track the security incident. Executive management at AWS receives updates on all data security investigations. In the event there are positive indicators for all steps in the security incident protocol, a security engineer engages the AWS CISO and AWS Legal team for a security review. The CISO and Legal team review the evidence and determine if a data breach has occurred. If confirmed, affected customers are notified in accordance with their reporting agreements. The AWS Security Incident Response whitepaper includes guidance on performing forensics on the AWS platform. Please refer to:	AWS

					https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf	

SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			AWS contingency plans and incident response playbooks have defined and tested tools and processes to detect, mitigate, investigate, and report a security incident. It includes guidelines for responding to and reporting a data breach in accordance with customer agreements. AWS security engineers follow a protocol when responding to a data security incident. The protocol involves steps which include validating customer data existence within the AWS service, determining the encryption status of a customer's content, and determining unauthorized access to a customer's content to the extent able. If any step in the event does not reveal a positive indicator, the security engineer documents the findings in internal tools used to track the security incident. Executive management at AWS receives updates on all data security investigations. In the event there are positive indicators for all steps in the security incident protocol, a security engineer engages the AWS CISO and AWS Legal team for a security review. The CISO and Legal team review the evidence and determine if a data breach has occurred. If confirmed, affected customers are notified in accordance with their reporting agreements. The AWS Security Incident Response whitepaper includes guidance on performing forensics on the AWS platform. Please refer to:	AWS

					https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf	

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			Customers retain control over their content on the AWS platform, including the ability to preserve logs, snapshots, and other evidence by copying them to a centralized security cloud account. As well as native AWS features, Customers are free to use their own mechanisms, for example, you may choose to use Linux dd command or a Windows equivalent to make a complete copy of data for investigative purposes.	Customer
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			Amazon does not disclose customer information unless we're required to do so to comply with a legally valid and binding order. Unless 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 content information. Amazon makes public its compliance with information requests on a six-month basis in its public Information Request Report, which can be found at the included link: https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			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
SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?		X		AWS tracks detail metrics for internal process measurements and improvements, but this level of detail is not shared, as it constitutes internal proprietary information.	N/A
STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?		X		Customers retain control and ownership over the quality of their data and potential quality errors that may arise through their usage of AWS services. Refer to AWS SOC report for specific details in relation to Data Integrity and Access Management (including least privilege access).	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X			AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards. AWS maintains standard contract review and signature processes that include legal reviews with consideration of protecting AWS resources. AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. Depending on contract requirements, AWS maintains procedures for notifying customers of customer-impacting issues using the AWS Service Health Dashboard (available at http://status.aws.amazon.com/). The AWS SOC reports provide details on the specific control activities executed by AWS. In addition, the AWS: Overview of Security Processes Whitepaper provides further details - available at: http://aws.amazon.com/security/security-learning/	AWS
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			AWS continuously monitors service usage to project infrastructure needs to support availability commitments and requirements. AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-03.2	Do you provide tenants with capacity planning and use reports?	X			AWS monitors customers usage of AWS resources to enable appropriate billing of customers. Customers can view their usage reports for their own billing and capacity planning purposes on: https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/ AWS does not disclose capacity planning reports for usage across all customers.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			As its third line of defense, AWS employs an Internal Audit function with due professional care to periodically evaluate risks and assess conformance to AWS security processes. Further, independent assurance is also provided by AWS Compliance teams (such as the Incident Management, Vulnerability Assessments, penetration testing teams) or by independent third-party assessors. These assessors provide an independent assessment of risk management content/processes by performing periodic security assessments and compliance audits or examinations (e.g. SOC, ISO, PCI audits) to evaluate the security, integrity, confidentiality, and availability of information and resources. AWS management also collaborates with Internal Audit to determine the health of the AWS control environment, and leverages this information to fairly present the assertions made within the report.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			Through the use of established assessment procedures, AWS assesses and continuously monitors suppliers to ensure that they are conforming to specific AWS requirements and contractual obligations. The extent of assessment for a supplier is dependent upon the significance of the product and/or service purchased and, where applicable, upon previously demonstrated performance.	AWS
STA-05.2	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X			Through the use of established assessment procedures, AWS assesses and continuously monitors suppliers to ensure that they are conforming to specific AWS requirements and contractual obligations. The extent of assessment for a supplier is dependent upon the significance of the product and/or service purchased and, where applicable, upon previously demonstrated performance.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-05.3	Does legal counsel review all third-party agreements?	X			AWS creates and maintains written contracts with third parties (for example, Contractors or vendors) in accordance with the work or service to be provided (for example, network services agreement, service delivery agreement, or information exchange agreement) and implements appropriate relationship management mechanisms in line with their relationship to the business. Contracts with significant suppliers that provide services to AWS must go through the standard contract review process. The contract is reviewed by the AWS legal team to ensure there is proper legal protection over AWS resources. Contractors who assist AWS must follow the agreed upon logical security controls and there is a process to monitor and evaluate contractors who are assisting critical AWS functions.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	X			Contracts with third-party suppliers cover, at a minimum, the following: • Legal and regulatory requirements applicable to AWS • User awareness of information security responsibilities and issues • Arrangements for reporting, notification, and investigation of information security incidents and security breaches • Target and unacceptable levels of service (for example, SLA, OLA) • Service continuity requirements (e.g., recovery time objectives - RTO), in accordance with AWS business priorities • Protection of Intellectual Property Rights (IPR) and copyright assignment of AWS • Conditions for renegotiation/termination of the agreement AWS' third party management processes include periodic contract review and reporting, and are reviewed by independent auditors.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 and Glacier services are designed to reduce the likelihood of data loss and provide durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS website.	Shared
STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-05.7	Can you provide the physical location/geography of storage of a tenant's data upon request?	X			AWS provides customers the flexibility to place instances and store data within multiple geographic Regions. AWS Customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.	Customer
STA-05.8	Can you provide the physical location/geography of storage of a tenant's data in advance?	X			AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-05.9	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	X			AWS provides customers the flexibility to place instances and store data within multiple geographic regions. AWS Customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.	Customer
STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?			X	AWS Customers retain the responsibility to monitor their own environment for privacy breaches. AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored. The AWS SOC reports provide an overview of the controls in place to monitor AWS managed environment.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		X		AWS tenants cannot opt out of mandatory metadata collected to perform customer billing. AWS Artificial Intelligence (AI) services may use and store AI content as outlined in Service Terms agreement. The Agreement also outlines the "opt-out" options available to customers.	N/A
STA-05.12	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		X		AWS may engage the entities listed on the AWS Sub-Processors website: (https://aws.amazon.com/compliance/sub-processors/) to carry out specific processing activities on behalf of the customer or datacenter facility management activities pursuant to the AWS Data Processing Addendum (https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf). This website also provides customers with the option to subscribe to email notifications if the list of sub-processors changes.	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	X			AWS maintains a formal risk management policy and procedures which includes management and assessment of risks posed by subcontractors. AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/	AWS
STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X			Through the use of established assessment procedures, AWS assesses and continuously monitors suppliers to ensure that they are conforming to specific AWS requirements. The extent of assessment for a supplier is dependent upon the significance of the product and/or service purchased and, where applicable, upon previously demonstrated performance.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?			X	AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/	N/A
STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?			X	AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			Current AWS SLAs can be found here: https://aws.amazon.com/legal/service-level-agreements/	AWS
STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	X			AWS CloudWatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to: http://aws.amazon.com/CloudWatch for additional details.	AWS
STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			AWS publishes current information on service availability on the Service Health Dashboard. Refer to AWS Service Health Dashboard: https://status.aws.amazon.com/	AWS
STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?			X	This question is not relevant to services provided by AWS.	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-07.8	Do you review all service level agreements at least annually?	X			SLAs are reviewed periodically. Current AWS SLAs can be found here: https://aws.amazon.com/legal/service-level-agreements/	AWS
STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?			X	AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?			X	AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards. AWS maintains standard contract review and signature processes that include legal reviews with consideration of protecting AWS resources. AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	X			AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards. AWS maintains standard contract review and signature processes that include legal reviews with consideration of protecting AWS resources. AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to: https://aws.amazon.com/compliance/third-party-access/	AWS
STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			AWS Security regularly engages carefully selected industry experts and independent security firms to perform recurring penetration testing, however, we do not share the results directly with customers. Instead, the results are reviewed and validated by our auditors.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	X			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.	AWS
TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X			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.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools.	AWS

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?			X	Customers retain control of their own guest operating systems, software and applications and are responsible for performing vulnerability scans and patching of their own systems. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. AWS Security regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers. 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.	Customer

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?			X	Customers retain control of their own guest operating systems, software and applications and are responsible for performing vulnerability scans and patching of their own systems. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. AWS Security regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers. 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.	Customer
TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?		X		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.	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools. Customers are responsible for maintaining the application of patches to their Amazon instances.	Shared
TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?			X	Customer data is not used as part of AWS service. Customer notification responsibilities are mutually agreed per contracts. AWS Services terms are available at https://aws.amazon.com/service-terms/	N/A

Question ID	Consensus Assessment Questions	Answer			Notes	Control Responsibility
		Yes	No	N/A		
TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	AWS allows customers to manage client and mobile applications to their own requirements.	N/A
TVM-03.2	Is all unauthorized mobile code prevented from executing?			X	AWS allows customers to manage client and mobile applications to their own requirements.	N/A

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
February 2020	Updated CAIQ template and updated responses to individual questions.
July 2018	2018 validation and update
January 2018	Migrated to new template.
January 2016	First publication