Amazon Web Services: Risk and Compliance

January 2013

(Please consult http://aws.amazon.com/security for the latest version of this paper)

This document intends to provide information to assist AWS customers with integrating AWS into their existing control framework supporting their IT environment. This document includes a basic approach to evaluating AWS controls and provides information to assist customers with integrating control environments. This document also addresses AWS-specific information around general cloud computing compliance issues.

This document provides the following:

Risk and Compliance Overview

Since AWS and its customers share control over the IT environment, both parties have responsibility for managing the IT environment. AWS' part in this shared responsibility includes providing its services on a highly secure and controlled platform and providing a wide array of security features customers can use. The customers' responsibility includes configuring their IT environments in a secure and controlled manner for their purposes. While customers don't communicate their use and configurations to AWS, AWS does communicate its security and control environment relevant to customers. AWS does this by doing the following:

- Obtaining industry certifications and independent third party attestations described in this document
- Publishing information about the AWS security and control practices in whitepapers and web site content
- Providing certificates, reports, and other documentation directly to AWS customers under NDA (as required)

Please see the AWS Security Whitepaper, located at www.aws.amazon.com/security, for a more detailed description of AWS security. The AWS Security Whitepaper covers AWS's general security controls and service-specific security.

Shared Responsibility Environment

Moving IT infrastructure to AWS services creates a model of shared responsibility between the customer and AWS. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. It is possible for customers to enhance security and/or meet their more stringent compliance requirements by leveraging technology such as host based firewalls, host based intrusion detection/prevention, encryption and key management. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment of solutions that meet industry-specific certification requirements.

This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls shared. AWS can help relieve customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them (described in the "AWS Certifications and Third-party Attestations" section of this document) to perform their control evaluation and verification procedures as required.

The next section provides an approach on how AWS customers can evaluate and validate their distributed control environment effectively.

Strong Compliance Governance

As always, AWS customers are required to continue to maintain adequate governance over the entire IT control environment regardless of how IT is deployed. Leading practices include an understanding of required compliance objectives and requirements (from relevant sources), establishment of a control environment that meets those objectives and requirements, an understanding of the validation required based on the organization's risk tolerance, and verification of the operating effectiveness of their control environment. Deployment in the AWS cloud gives enterprises different options to apply various types of controls and various verification methods.

Strong customer compliance and governance might include the following basic approach:

1. Review information available from AWS together with other information to understand as much of the entire IT environment as possible, and then document all compliance requirements.
2. Design and implement control objectives to meet the enterprise compliance requirements.
3. Identify and document controls owned by outside parties.
4. Verify that all control objectives are met and all key controls are designed and operating effectively.

Approaching compliance governance in this manner will help companies gain a better understanding of their control environment and will help clearly delineate the verification activities to be performed.

Evaluating and Integrating AWS Controls

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, and other third-party attestations. This documentation assists customers in understanding the controls in place relevant to the AWS services they use and how those controls have been validated. This information also assists customers in their efforts to account for and to validate that controls in their extended IT environment are operating effectively.

Traditionally, the design and operating effectiveness of control objectives and controls are validated by internal and/or external auditors via process walkthroughs and evidence evaluation. Direct observation/verification—by the customer or customer's external auditor—is generally performed to validate controls. In the case where service providers, such as AWS, are used, companies request and evaluate third-party attestations and certifications in order to gain reasonable assurance of the design and operating effectiveness of control objective and controls. As a result, although customer's key controls may be managed by AWS, the control environment can still be a unified framework where all controls are accounted for and are verified as operating effectively. Third-party attestations and certifications of AWS can not only provide a higher level of validation of the control environment, but may relieve customers of the requirement to perform certain validation work themselves for their IT environment in the AWS cloud.

AWS provides IT control information to customers in the following two ways:

1. **Specific control definition.** AWS customers are able to identify key controls managed by AWS. Key controls are critical to the customer's control environment and require an external attestation of the operating effectiveness of these key controls in order to comply with compliance requirements—such as the annual financial audit. For this purpose, AWS publishes a wide range of specific IT controls in its Service Organization Controls 1 (SOC 1) Type II report. The SOC 1 report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report and commonly referred to as the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) report, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SOC 1 audit is an in-depth audit of both the design and operating effectiveness of AWS' defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). "Type II" refers to the fact that each of the controls described in the report are not only evaluated for adequacy of design, but are also tested for operating effectiveness by the external auditor. Because of the independence and competence of AWS' external auditor, controls identified in the report should provide customers with a high level of confidence in AWS' control environment. AWS' controls can be considered designed and operating effectively for many compliance purpose, including Sarbanes-Oxley (SOX) Section 404 financial statement audits. Leveraging SOC 1 Type II reports is also generally permitted by other external certifying bodies (e.g., ISO 27001 auditors may request a SOC 1 Type II report in order to complete their evaluations for customers).

Other specific control activities relate to AWS' Payment Card Industry (PCI) and Federal Information Security Management Act (FISMA) compliance. As discussed below, AWS is compliant with FISMA Moderate standards and with the PCI Data Security Standard. These PCI and FISMA standards are very prescriptive and require independent validation that AWS adheres to the published standard.

2. **General control standard compliance.** If an AWS customer requires a broad set of control objectives to be met, evaluation of AWS' industry certifications may be performed. With the AWS ISO 27001 certification, AWS complies with a broad, comprehensive security standard and follows best practices in maintaining a secure environment. With the PCI Data Security Standard (PCI DSS), AWS complies with a set of controls important to companies that handle credit card information. With AWS' compliance with the FISMA standards, AWS complies with a wide range of specific controls required by US government agencies. Compliance with these general standards provides customers with in-depth information on the comprehensive nature of the controls and security processes in place and can be considered when managing compliance.

AWS certifications and third party attestations are discussed in more detail later in this document.

AWS Risk and Compliance Program

AWS provides information about its risk and compliance program to enable customers to incorporate AWS controls into their governance framework. This information can assist customers in documenting a complete control and governance framework with AWS included as an important part of that framework.

Risk Management

AWS management has developed 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.

In addition, the AWS control environment is subject to various internal and external risk assessments. AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, the PCI DSS, and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems). AWS maintains the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy.

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. These scans are done in a manner for the health and viability of the underlying AWS infrastructure and are not meant to replace the customer's own vulnerability scans required to meet their specific compliance requirements. 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. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form.

AWS Control Environment

AWS manages a comprehensive control environment that includes policies, processes and control activities that leverage various aspects of Amazon's overall control environment. This control environment is in place for the secure delivery of AWS' service offerings. The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of AWS' control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS continues to monitor these industry groups for ideas on which leading practices can be implemented to better assist customers with managing their control environment.

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.

The AWS organizational structure provides a framework for planning, executing and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel. Included as part of the Company's hiring verification processes are education, previous employment, and, in some cases, background checks as permitted by law and regulation. The Company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, policies and procedures.

Information Security

AWS has implemented a formal information security program designed to protect the confidentiality, integrity, and availability of customers' systems and data. AWS publishes a security whitepaper that is available on the public website that addresses how AWS can help customers secure their data.

AWS Certifications and Third-party Attestations

AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS.

SOC 1/SSAE 16/ISAE 3402

Amazon Web Services now publishes a Service Organization Controls 1 (SOC 1), Type II report. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) professional standards. This dual-standard report is intended to meet a broad range of financial auditing requirements for U.S. and international auditing bodies. The SOC 1 report audit attests that AWS' control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II Audit report.

The AWS SOC 1 control objectives are provided here. The report itself identifies the control activities that support each of these objectives and the independent auditor's results of their testing procedures of each control.

Security Organization	Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.
Amazon User Access	Controls provide reasonable assurance that procedures have been established so that Amazon user accounts are added, modified and deleted in a timely manner and are reviewed on a periodic basis.
Logical Security	Controls provide reasonable assurance that unauthorized internal and external access to data is appropriately restricted and access to customer data is appropriately segregated from other customers.
Secure Data Handling	Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.
Physical Security and Environmental Safeguards	Controls provide reasonable assurance that physical access to Amazon's operations building and the data centers is restricted to authorized personnel and that procedures exist to minimize the effect of a malfunction or physical disaster to the computer and data center facilities.
Change Management	Controls provide reasonable assurance that changes (including emergency / non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.

Data Integrity, Availability and Redundancy	Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.
Incident Handling	Controls provide reasonable assurance that system incidents are recorded, analyzed, and resolved.

The new SOC 1 reports are designed to focus on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. As AWS' customer base is broad, and the use of AWS services is equally as broad, the applicability of controls to customer financial statements varies by customer. Therefore, the AWS SOC 1 report is designed to cover specific key controls likely to be required during a financial audit, as well as covering a broad range of IT general controls to accommodate a wide range of usage and audit scenarios. This allows customers to leverage the AWS infrastructure to store and process critical data, including that which is integral to the financial reporting process. AWS periodically reassesses the selection of these controls to consider customer feedback and usage of this important audit report.

AWS' commitment to the SOC 1 report is on-going, and AWS will continue the process of periodic audits. The SOC 1 report scope covers Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Virtual Private Cloud (VPC), Amazon Elastic Block Store (EBS), Amazon Relational Database Service (RDS), Amazon DynamoDB, Amazon SimpleDB, Amazon Direct Connect, Amazon VM Import/Export, Amazon ElastiCache, Amazon Glacier, Amazon Storage Gateway and the infrastructure upon which they run for all regions worldwide, including the Amazon GovCloud (US) region.

SOC 2

In addition to the SOC 1 report, AWS publishes a Service Organization Controls 2 (SOC 2), Type 2 report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security principle set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security based on a pre-defined industry standard of leading practices and further demonstrates AWS' commitment to protecting customer data.

The SOC 2 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services.

FISMA, DIACAP, and FedRAMP

AWS enables US government agencies to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). The AWS infrastructure has been evaluated by independent assessors for a variety of government systems as part of their system owners' approval process. Numerous Federal Civilian and Department of Defense (DoD) organizations have successfully achieved security authorizations for systems hosted on the AWS cloud in accordance with the Risk Management Framework (RMF) process defined in NIST 800-37 and DoD Information Assurance Certification and Accreditation Process (DIACAP). AWS's secure infrastructure has helped federal agencies expand cloud computing use cases and deploy sensitive government data and applications in the cloud while complying with the rigorous security requirements of federal standards.

The Federal Risk and Authorization Management Program (FedRAMP) is a government program designed to standardize security assessment, authorization, and continuous monitoring for cloud services. AWS operates a FedRAMP compliance program and is currently working with an authorized Third Party Assessment Organization (3PAO), the FedRAMP office, and other US government agencies in achieving compliance with FedRAMP requirements.

PCI DSS Level 1

AWS satisfies the requirements under PCI DSS for shared hosting providers. AWS also has been successfully validated against standards applicable to a Level 1 service provider under PCI DSS Version 2.0. Merchants and other PCI service providers can use the AWS PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud, as long as those customers create PCI compliance for their part of the shared environment. This compliance validation includes Amazon EC2, Amazon S3, Amazon EBS, Amazon VPC, Amazon RDS, Amazon Elastic Load Balancing (ELB), Amazon Identity and Access Management (IAM), and the infrastructure upon which those services run for all regions worldwide. AWS provides additional information and frequently asked questions about its PCI compliance on its web site and works with customers directly on preparing for and deploying a PCI-compliant cardholder environment on AWS infrastructure.

ISO 27001

AWS has achieved ISO 27001 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services including Amazon EC2, Amazon S3 and Amazon VPC. ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments appropriate to ever-changing threat scenarios. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This certification reinforces Amazon's commitment to providing significant information regarding our security controls and practices. AWS's ISO 27001 certification includes all AWS data centers in all regions worldwide and AWS has established a formal program to maintain the certification. AWS provides additional information and frequently asked questions about its ISO 27001 certification on their web site.

International Traffic in Arms Regulations

The AWS GovCloud (US) region offered by AWS supports US International Traffic in Arms Regulations (ITAR) compliance. As a part of managing a comprehensive ITAR compliance program, companies subject to ITAR export regulations must control unintended exports by restricting access to protected data to US persons and restricting physical location of that data to US land. AWS GovCloud (US) provides an environment physically located in the US and where access by AWS Personnel is limited to US persons and, thereby allows qualified companies to transmit, process, and store protected articles and data under ITAR. The AWS GovCloud (US) environment has been audited by an independent third party to validate the proper controls are in place to support customer export compliance programs for this requirement.

FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, the Amazon Virtual Private Cloud VPN endpoints and SSL-terminating load balancers in AWS GovCloud (US) operate using FIPS 140-2 validated hardware. AWS works with AWS GovCloud (US) customers to provide the information they need to help manage compliance with this requirement when using the AWS GovCloud (US) environment.

Other Compliance Initiatives

The flexibility and customer control that the AWS platform provides permits the deployment of solutions that meet industry-specific compliance requirements.

- HIPAA: Customers have built healthcare applications compliant with HIPAA's Security and Privacy Rules on AWS. AWS provides the security controls customers can use to help to secure electronic health records. Please see the related whitepaper at http://aws.amazon.com/security.

- CSA: AWS has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire. This questionnaire published by the CSA provides a way to reference and document what security controls exist in AWS's Infrastructure-as-a-Service offerings. The questionnaire (CAIQ) provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. See Appendix A of this document for the CSA Consensus Assessments Initiative Questionnaire completed by AWS.
- MPAA: The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content (http://www.fightfilmtheft.org/facility-security-program.html). Media companies use these best practices as a way to assess risk and security of their content and infrastructure. AWS has demonstrated alignment with the MPAA best practices and the AWS infrastructure is compliant with all applicable MPAA infrastructure controls. While the MPAA does not offer a "certification," media industry customers can use the AWS MPAA documentation to augment their risk assessment and evaluation of MPAA-type content on AWS. See Appendix B of this document for the AWS alignment with Motion Picture of America Association (MPAA) Content Security Model.

Key Compliance Issues and AWS

This section addresses generic cloud computing compliance issues specifically for AWS. These common compliance issues listed may be of interest when evaluating and operating in a cloud computing environment and may assist in AWS customers' control management efforts.

Ref	Cloud Computing Issue Topic	AWS Information
1	Control ownership. Who owns which controls for cloud-deployed infrastructure?	For the portion deployed into AWS, AWS controls the physical components of that technology. The customer owns and controls everything else, including control over connection points and transmissions. To help customers better understand what controls we have in place and how effectively they are operating, we publish a SOC 1 Type II report with controls defined around EC2, S3 and VPC, as well as detailed physical security and environmental controls. These controls are defined at a high level of specificity that should meet most customer needs. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report.
2	Auditing IT. How can auditing of the cloud provider be accomplished?	Auditing for most layers and controls above the physical controls remains the responsibility of the customer. The definition of AWS-defined logical and physical controls is documented in the SOC 1 Type II report (SSAE 16), and the report is available for review by audit and compliance teams. AWS ISO 27001 and other certifications are also available for auditors to review.
3	Sarbanes-Oxley compliance. How is SOX compliance achieved if in-scope systems are deployed in the cloud provider environment?	If a customer processes financial information in the AWS cloud, the customer's auditors may determine that some AWS systems come into scope for Sarbanes-Oxley (SOX) requirements. The customer's auditors must make their own determination regarding SOX applicability. Because most of the logical access controls are managed by customer, the customer is best positioned to determine if its control activities meet relevant standards. If the SOX auditors request specifics regarding AWS' physical controls, they can reference AWS' SOC 1 Type II report which details the controls that AWS provides.
4	HIPAA compliance. Is it possible to meet HIPAA compliance requirements while deployed in the cloud provider environment?	HIPAA requirements apply to and are controlled by the AWS customer. The AWS platform allows for the deployment of solutions that meet industry-specific certification requirements such as HIPAA. Customers can use AWS services to maintain a security level that is equivalent or greater than those required to protect electronic health records. Customers have built healthcare applications compliant with HIPAA's Security and Privacy Rules on AWS. AWS provides additional information about HIPAA compliance on its web site, including a whitepaper on this topic.

5	GLBA compliance. Is it possible to meet GLBA certification requirements while deployed in the cloud provider environment?	Most GLBA requirements are controlled by the AWS customer. AWS provides means for customers to protect data, manage permissions, and build GLBA-compliant applications on AWS infrastructure. If the customer requires specific assurance that physical security controls are operating effectively, they can reference the AWS SOC 1 Type II report as relevant.
6	Federal regulation compliance. Is it possible for a US Government agency to be compliant with security and privacy regulations while deployed in the cloud provider environment?	US Federal agencies can be compliant under a number of compliance standards, including the Federal Information Security Management Act (FISMA) of 2002, the Federal Information Processing Standard (FIPS) Publication 140-2, and the International Traffic in Arms Regulations (ITAR). Compliance with other laws and statues may also be accommodated depending on the requirements set forth in the applicable legislation.
7	Data location. Where does customer data reside?	AWS customers designate in which physical region their data and their servers will be located. Data replication for S3 data objects is done within the regional cluster in which the data is stored and is not replicated to other data center clusters in other 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. AWS currently offers eight regions: US East (Northern Virginia), US West (Northern California), US West (Oregon), GovCloud (US) (Oregon), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), and South America (Sao Paulo).
8	E-Discovery. Does the cloud provider meet the customer's needs to meet electronic discovery procedures and requirements?	AWS provides infrastructure, and customers manage everything else, including the operating system, the network configuration, and the installed applications. Customers are responsible for responding appropriately to legal procedures involving the identification, collection, processing, analysis, and production of electronic documents they store or process using AWS. Upon request, AWS may work with customers who require AWS' assistance in legal proceedings.
9	Data center tours. Are data center tours by customers allowed by the cloud provider?	No. Due to the fact that our datacenters host multiple customers, AWS does not allow datacenter tours by customers, as this exposes a wide range of customers to physical access of a third party. To meet this customer need, an independent and competent auditor validates the presence and operation of controls as part of our SOC 1 Type II report (SSAE 16). This broadly accepted third-party validation provides customers with the independent perspective of the effectiveness of controls in place. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report. Independent reviews of data center physical security is also a part of the ISO 27001 audit, the PCI assessment, ITAR audit, and the FISMA testing programs.

10	Third party access. Are third parties allowed access to the cloud provider data centers?	AWS strictly controls access to data centers, even for internal employees. Third parties are not provided access to AWS data centers except when explicitly approved by the appropriate AWS datacenter manager per AWS' access policy. See the SOC 1 Type II report for specific controls related to physical access, datacenter access authorization, and other related controls.
11	Privileged actions. Are privileged actions monitored and controlled?	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 is and server instances are logically isolated from other customers by default. Privileged user access control is reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, ITAR, and FISMA audits.
12	Insider access. Does the cloud provider address the threat of inappropriate insider access to customer data and applications?	AWS provides specific SOC 1 controls to address the threat of inappropriate insider access, and the public certification and compliance initiatives covered in this document address 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.
13	Multi-tenancy. Is customer segregation implemented securely?	The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 2.0 published in October 2010. Note that AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within your Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS cloud while isolating your Amazon EC2 compute instances at the hardware level.
14	Hypervisor vulnerabilities. Has the cloud provider addressed known hypervisor vulnerabilities?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. See the AWS security whitepaper for more information on the Xen hypervisor and instance isolation.

15	Vulnerability management. Are systems patched appropriately?	AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. Customers control their own guest operating systems, software and applications and are therefore responsible for patching their own systems.
16	Encryption. Do the provided services support encryption?	Yes. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB, and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. Please see the AWS Security white paper for more information.
17	Data ownership. What are the cloud provider's rights over customer data?	AWS customers retain control and ownership of their data. AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis.
18	Data isolation. Does the cloud provider adequately isolate customer data?	All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Amazon S3 provides advanced data access controls. Please see the AWS security whitepaper for more information about specific data services' security.
19	Composite services. Does the cloud provider layer its service with other providers' cloud services?	AWS does not leverage any third-party cloud providers to deliver AWS services to customers.
20	Physical and environmental controls. Are these controls operated by the cloud provider specified?	Yes. These are specifically outlined in the SOC 1 Type II report. In addition, other certifications AWS supports such as ISO 27001 and FISMA require best practice physical and environmental controls.
21	Client-side protection. Does the cloud provider allow customers to secure and manage access from clients, such as PC and mobile devices?	Yes. AWS allows customers to manage client and mobile applications to their own requirements.
22	Server security. Does the cloud provider allow customers to secure their virtual servers?	Yes. AWS allows customers to implement their own security architecture. See the AWS security whitepaper for more details on server and network security.

23	Identity and Access Management. Does the service include IAM capabilities?	AWS has a suite of identity and access management offerings, allowing customers to manage user identities, assign security credentials, organize users in groups, and manage user permissions in a centralized way. Please see the AWS web site for more information.
24	Scheduled maintenance outages. Does the provider specify when systems will be brought down for maintenance?	AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS's own maintenance and system patching generally do not impact customers. Maintenance of instances themselves is controlled by the customer.
25	Capability to scale. Does the provider allow customers to scale beyond the original agreement?	The AWS cloud is distributed, highly secure and resilient, giving customers massive scale potential. Customers may scale up or down, paying for only what they use.
26	Service availability. Does the provider commit to a high level of availability?	AWS does commit to high levels of availability in its service level agreements (SLA). For example, Amazon EC2 commits to annual uptime percentage of at least 99.95% during the service year. Amazon S3 commits to monthly uptime percentage of at least 99.99%. Service credits are provided in the case these availability metrics are not met. On April 21, 2011, EC2 suffered a customer-impacting service disruption in the US East Region. Details about the service disruption are described in "Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region" (http://aws.amazon.com/message/65648/).
27	Distributed Denial Of Service (DDoS) attacks. How does the provider protect their service against DDoS attacks?	The AWS network provides significant protection against traditional network security issues and the customer can implement further protection. See the AWS Security Whitepaper for more information on this topic, including a discussion of DDoS attacks.
28	Data portability. Can the data stored with a service provider be exported by customer request?	AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport.
29	Service provider business continuity. Does the service provider operate a business continuity program?	AWS does operate a business continuity program. Detailed information is provided in the AWS Security Whitepaper.

30	Customer business continuity. Does the service provider allow customers to implement a business continuity plan?	AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures.
31	Data durability. Does the service specify data durability?	Amazon S3 provides a highly durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. Once stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. Data stored in S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.
32	Backups. Does the service provide backups to tapes?	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 service is designed to drive the likelihood of data loss to near zero percent and the 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 web site.
33	Price increases. Will the service provider raise prices unexpectedly?	AWS has a history of frequently reducing prices as the cost to provide these services reduces over time. AWS has reduced prices consistently over the past several years.
34	Sustainability. Does the service provider company have long term sustainability potential?	AWS is a leading cloud provider and is a long-term business strategy of Amazon.com. AWS has very high long term sustainability potential.

AWS Contact

Customers can contact the AWS Compliance or Security team through their business development representative. The representative will route customers to the proper team depending on nature of the inquiry. Alternatively, general questions can be mailed to: aws-security@amazon.com

APPENDIX A – CSA CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE V1.1

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." [Reference https://cloudsecurityalliance.org/about/] A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission.

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.

Domain	Control Group	CID	Consensus Assessment Questions	AWS Response
Compliance	Audit Planning	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	AWS obtains certain industry certifications and independent third party attestations and provides certain certifications, reports and other relevant documentation directly to AWS customers under NDA.
Compliance	Independent Audits	CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?	AWS provides third party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. 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.
Compliance		CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	
Compliance		CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?	
Compliance		CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	
Compliance		CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	
Compliance		CO-02.6	Are the results of the network penetration tests available to tenants at their request?	
Compliance		CO-02.7	Are the results of internal and external audits available to tenants at their request?	
Compliance	Third Party Audits	CO-03.1	Do you permit tenants to perform independent vulnerability assessments?	Customers can request permission to conduct scans of their cloud infrastructure as long as they

Compliance		CO-03.2	Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?	are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form. AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS.
Compliance	Contact / Authority Maintenance	CO-04.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	AWS maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard.
Compliance	Information System Regulatory Mapping	CO-05.1	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?	All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
		CO-05.2	Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?	
Compliance	Intellectual Property	CO-06.1	Do you have policies and procedures in place describing what controls you have in place to protect tenant's intellectual property?	AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework. The AWS security framework integrates the ISO 27002 best practices and the PCI Data Security Standard. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
Compliance	Intellectual Property	CO-07.1	If utilization of tenants services housed in the cloud is mined for cloud provider benefit, are the tenants IP rights preserved?	Resource utilization is monitored by AWS as necessary to effectively manage the availability of the service. AWS does not collect customer's intellectual property as part of resource utilization monitoring.
Compliance	Intellectual Property	CO-08.1	If utilization of tenants services housed in the cloud is mined for cloud provider benefit, do you provide tenants the ability to opt-out?	Utilization of customer services housed in the cloud is not mined.
Data Governance	Ownership / Stewardship	DG-01.1	Do you follow a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	AWS customers retain control and ownership of their data and may implement a structured data-labeling standard to meet their requirements.

Data Governance	Classification	DG-02.1	Do you provide a capability to identify virtual machines via policy tags/metadata (ex. Tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country, etc.)?	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.
Data Governance		DG-02.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (ex. TXT/TPM, VN-Tag, etc.)?	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 has also supports tagging.
Data Governance		DG-02.3	Do you have a capability to use system geographic location as an authentication factor?	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.
Data Governance		DG-02.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	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. AWS currently offers six regions: US East (Northern Virginia), US West (Northern California and Oregon), GovCloud (US) (Oregon), South America (Sao Paulo), EU (Ireland), Asia Pacific (Singapore) and Asia Pacific (Tokyo). Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
Data Governance		DG-02.5	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	
Data Governance	Handling / Labeling / Security Policy	DG-03.1	Are Policies and procedures established for labeling, handling and security of data and objects which contain data?	AWS customers retain control and ownership of their data and may implement a labeling and handing policy and procedures to meet their requirements.
Data Governance		DG-03.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	
Data Governance	Retention Policy	DG-04.1	Do you have technical control capabilities to enforce tenant data retention policies?	AWS provide customers with the ability to delete their data. However, AWS customers retain control and ownership of their data so it is the customer's responsibility to manage data

Data Governance		DG-04.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	retention to their own requirements. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis.
Data Governance	Secure Disposal	DG-05.1	Do you support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the tenant?	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 DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Data Governance		DG-05.2	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?	
Data Governance	Nonproduction Data	DG-06.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	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.
Data Governance	Information Leakage	DG-07.1	Do you have controls in place to prevent data leakage or intentional/accidental compromise between tenants in a multi-tenant environment?	The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not

Data Governance		DG-07.2	Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?	assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 2.0 published in June 2011. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
Data Governance	Risk Assessments	DG-08.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status?)	AWS does publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS. The relevant certifications and reports can be provided to AWS customers. Continuous Monitoring of logical controls can be executed by customers on their own systems.
Facility Security	Policy	FS-01.1	Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	AWS engages with external certifying bodies and independent auditors to review and validate our compliance with compliance frameworks. AWS SOC 1 Type 2 report provides additional details on the specific physical security control activities executed by AWS. Refer to ISO 27001 standard, Annex A, domain 9.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Facility Security	User Access	FS-02.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?	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.
Facility Security	Controlled Access Points	FS-03.1	Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	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 1 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standard, Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Facility Security	Secure Area Authorization	FS-04.1	Do you allow tenants to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	AWS customers can designate 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. AWS currently offers six regions: US East (Northern Virginia), US West (Northern California and Oregon), GovCloud (US) (Oregon), South America (Sao Paulo), EU (Ireland), Asia Pacific (Singapore) and Asia Pacific (Tokyo). Refer to the AWS website at http://aws.amazon.com for additional details.
Facility Security	Unauthorized Persons Entry	FS-05.1	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?	Physical access is strictly controlled both at the perimeter and at building ingress points by 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 datacenter floors. Refer to AWS Overview of Security Processes Whitepaper for further information available at http://aws.amazon.com/security. In addition, the AWS SOC 1 type 2 report provides additional details on the specific control activities executed by AWS.
Facility Security	Offsite Authorization	FS-06.1	Do you provide tenants with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business continuity failovers, replication)	AWS customers can designate which physical region their data 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. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Facility Security	Offsite equipment	FS-07.1	Do you provide tenants with documentation describing your policies and procedures governing asset management and repurposing of equipment?	In alignment with ISO 27001 standards, 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 DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to ISO 27001 standard, Annex A, domain 9.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Facility Security	Asset Management	FS-08.1	Do you maintain a complete inventory of all of your critical assets which includes ownership of the asset?	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 procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Facility Security		FS-08.2	Do you maintain a complete inventory of all of your critical supplier relationships?	
Human Resources Security	Background Screening	HR-01.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?	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. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Human Resources Security	Employment Agreements	HR-02.1	Do you specifically train your employees regarding their role vs. the tenant's role in providing information security controls?	Every employee is provided with the Company's Code of Business Conduct and Ethics and completes 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.
		HR-02.2	Do you document employee acknowledgment of training they have completed?	
Human Resources Security	Employment Termination	HR-03.1	Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?	AWS Human Resources team defines internal management responsibilities to be followed for termination and role change of employees and vendors. The responsibility for provisioning /de-provisioning employee and contractor access is shared across Human Resources (HR), Corporate Operations and Service Owners. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Information Security	Management Program	IS-01.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	AWS provides our customers with our ISO 27001 certification documentation that communicates AWS ISMS program.
Information Security	Management Support / Involvement	IS-02.1	Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?	In alignment with ISO 27001 standards, policies and procedures have been established through AWS Information Security framework. 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. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.

Information Security	Policy	IS-03.1	Do your information security and privacy policies align with particular industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	Policies and procedures have been established by AWS Information Security based upon the COBIT framework, ISO 27001 standards and the PCI DSS requirements. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition AWS publishes a SOC 1 Type II report. Refer to the SOC 1 report for further details. The AWS Risk and Compliance whitepaper for additional details - available at http://aws.amazon.com/security.
		IS-03.2	Do you have agreements which ensure your providers adhere to your information security and privacy policies?	
		IS-03.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	
Information Security	Baseline Requirements	IS-04.1	Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?	In alignment with ISO 27001 standards, AWS maintains system baselines for critical components. Refer to ISO 27001 standard, Annex A, domain 12.1 and 15.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Customers can provide their own virtual machine image. VM Import enables customers to easily import virtual machine images from your existing environment to Amazon EC2 instances.
Information Security		IS-04.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	
Information Security		IS-04.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	
Information Security	Policy Reviews	IS-05.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	AWS Overview of Security Processes whitepaper and Risk and Compliance whitepapers, available at http://aws.amazon.com/security are updated on a regular basis to reflect updates to the AWS policies.
Information Security	Policy Enforcement	IS-06.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	AWS provides security policy and provides security training to employees to educate them as to their role and responsibilities concerning information security. Employees who violate Amazon standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed. Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. Refer to ISO 27001 Annex A, domain 8.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Information Security		IS-06.2	Are employees made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures?	

Information Security	User Access Policy	IS-07.1	Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?	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. The AWS SOC 1 Type II report provides 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 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Information Security		IS-07.2	Do you provide metrics which track the speed with which you are able to remove systems access which is no longer required for business purposes?	
Information Security	User Access Restriction / Authorization	IS-08.1	Do you document how you grant and approve access to tenant data?	AWS customers retain control and ownership of their data. Customers are responsible for the development, content, operation, maintenance, and use of their content.
Information Security		IS-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	
Information Security	User Access Revocation	IS-09.1	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 third parties?	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 1 Type II report provides 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 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Information Security		IS-09.2	Is any change in status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	
Information Security	User Access Reviews	IS-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	In alignment with ISO 27001 standard, all access grants are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically revoked. Controls specific to User Access reviews are outlined in the SOC 1 Type II report. Exceptions in the User entitlement controls are documented in the SOC 1 Type II report.
Information Security		IS-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	

Information Security		IS-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	Refer to ISO 27001 standard, Annex A, domain 11.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Information Security	Training / Awareness	IS-11.1	Do you provide or make available a formal security awareness training program for cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	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.
Information Security		IS-11.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	
Information Security	Industry Knowledge / Benchmarking	IS-12.1	Do you participate in industry groups and professional associations related to information security?	AWS Compliance and Security teams maintain contacts with industry groups and professional services related to security. AWS has established an information security framework and policies based upon the COBIT framework and have integrated the ISO 27001 certifiable framework based on ISO 27002 controls and the PCI DSS. Refer to the AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
		IS-12.2	Do you benchmark your security controls against industry standards?	
Information Security	Roles / Responsibilities	IS-13.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities vs. those of the tenant?	The AWS Overview of Security Processes 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.
Information Security	Management Oversight	IS-14.1	Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?	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/security.

Information Security	Segregation of Duties	IS-15.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Customers retain the ability to manage segregations of duties of their AWS resources. Internally, AWS aligns with ISO 27001 standard for managing segregation of duties. Refer to ISO 27001 standard, Annex A, domain 10.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Information Security	User Responsibility	IS-16.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	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 8.2 and 11.3. 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.
Information Security		IS-16.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	
Information Security		IS-16.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	
Information Security	Workspace	IS-17.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	AWS data management policies are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 8.2 and 11.3. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources.
Information Security		IS-17.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	
Information Security		IS-17.3	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?	
Information Security	Encryption	IS-18.1	Do you have a capability to allow creation of unique encryption keys per tenant?	AWS Customers manage their own encryption unless they are utilizing AWS server side encryption service. In this case, AWS does create a unique encryption key per tenant. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Information Security		IS-18.2	Do you support tenant generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate. (e.g. Identity based encryption)?	
Information Security	Encryption Key Management	IS-19.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. AWS key management procedures are in alignment with ISO 27001
Information Security		IS-19.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	

Information Security		IS-19.3	Do you have a capability to manage encryption keys on behalf of tenants?	standard. Refer to ISO 27001 standard, Annex A, domain 15.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Information Security		IS-19.4	Do you maintain key management procedures?	
Information Security	Vulnerability / Patch Management	IS-20.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	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's own maintenance and system patching generally do not impact customers. Refer to AWS Overview of Security Processes Whitepaper for further information - available at http://aws.amazon.com/security. Refer to ISO 27001 standard, Annex A, domain 12.5 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Information Security		IS-20.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	
Information Security		IS-20.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	
Information Security		IS-20.4	Will you make the results of vulnerability scans available to tenants at their request?	
Information Security		IS-20.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	
Information Security		IS-20.6	Will you provide your risk-based systems patching timeframes to your tenants upon request?	
Information Security	Antivirus / Malicious Software	IS-21.1	Do you have anti-malware programs installed on all systems which support your cloud service offerings?	AWS's program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC 1 Type 2 report provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 10.4 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Information Security		IS-21.2	Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?	
Information Security	Incident Management	IS-22.1	Do you have a documented security incident response plan?	AWS's incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS.
Information Security		IS-22.2	Do you integrate customized tenant requirements into your security incident response plans?	

Information Security		IS-22.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details.
Information Security	Incident Reporting	IS-23.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	AWS's incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Refer to the AWS Overview of Security Processes whitepaper and the AWS Risk & Compliance whitepaper (available at http://aws.amazon.com/security) for additional details.
Information Security		IS-23.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	
Information Security	Incident Response Legal Preparation	IS-24.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?	AWS's incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Refer to the AWS Overview of Security Processes whitepaper and the AWS Risk & Compliance whitepaper (available at http://aws.amazon.com/security) for additional details.
Information Security		IS-24.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	
Information Security		IS-24.3	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?	
Information Security		IS-24.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	
Information Security	Incident Response Metrics	IS-25.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	AWS Security Metrics are monitored and analyzed in accordance with ISO 27001 standard. Refer to ISO 27001 Annex A, domain 13.2 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Information Security		IS-25.2	Will you share statistical information security incident data with your tenants upon request?	
Information Security	Acceptable Use	IS-26.1	Do you provide documentation regarding how you may utilize or access tenant data and/or metadata?	AWS customers retain control and ownership of their data.
Information Security		IS-26.2	Do you collect or create metadata about tenant data usage through the use of inspection technologies (search engines, etc.)?	
Information Security		IS-26.3	Do you allow tenants to opt-out of having their data/metadata accessed via inspection technologies?	

Information Security	Asset Returns	IS-27.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	AWS customers retain the responsibility to monitor their own environment for privacy breaches. AWS SOC 1 Type 2 report provides an overview of the controls in place to monitor AWS managed environment.
Information Security		IS-27.2	Is your Privacy Policy aligned with industry standards?	
Information Security	eCommerce Transactions	IS-28.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)	All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Information Security		IS-28.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?	
Information Security	Audit Tools Access	IS-29.1	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	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 1 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security.
Information Security	Diagnostic / Configuration Ports Access	IS-30.1	Do you utilize dedicated secure networks to provide management access to your cloud service infrastructure?	Administrators with a business need to access the management plane are required to use multifactor authentication 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 of the cloud. 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.
Information Security	Network / Infrastructure Services	IS-31.1	Do you collect capacity and utilization data for all relevant components of your cloud service offering?	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.
Information Security		IS-31.2	Do you provide tenants with capacity planning and utilization reports?	

Information Security	Portable / Mobile Devices	IS-32.1	Are Policies and procedures established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as 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)?	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 1 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
Information Security	Source Code Access Restriction	IS-33.1	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?	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 1 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
Information Security		IS-33.2	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?	
Information Security	Utility Programs Access	IS-34.1	Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?	In alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored. AWS SOC 1 Type 2 report provides additional details on controls in place to restrict system access. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
Information Security		IS-34.2	Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)?	
Information Security		IS-34.3	Are attacks which target the virtual infrastructure prevented with technical controls?	
Legal	Nondisclosure Agreements	LG-01.1	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?	Amazon Legal Counsel manages and periodically revises the Amazon NDA to reflect AWS business needs.
Legal	Third Party Agreements	LG-02.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed and stored and transmitted?	AWS does not leverage any third-party cloud providers to deliver AWS services to customers. Third party agreements are reviewed by Amazon Legal Counsel as appropriate.
Legal		LG-02.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	
Legal		LG-02.3	Does legal counsel review all third party agreements?	

Operations Management	Policy	OP-01.1	Are policies and procedures established and made available for all personnel to adequately support services operations roles?	Policies and Procedures have been established through AWS Information Security framework based upon the COBIT framework, ISO 27001 standard and the PCI DSS requirements. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
Operations Management	Documentation	OP-02.1	Are Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure Configuring, installing, and operating the information system?	Information System Documentation is made available internal to AWS personnel through the use of Amazon's Intranet site. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Operations Management	Capacity / Resource Planning	OP-03.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	AWS does not disclose capacity management practices. AWS publishes service level agreements for services to communicate performance level commitments.
Operations Management		OP-03.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	
Operations Management	Equipment Maintenance	OP-04.1	If using virtual infrastructure, does your cloud solution include hardware independent restore and recovery capabilities?	EBS Snapshot functionality allows customers to capture and restore virtual machine images at any time. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Operations Management		OP-04.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	
Operations Management		OP-04.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	
Operations Management		OP-04.4	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?	
Operations Management		OP-04.5	Does your cloud solution include software / provider independent restore and recovery capabilities?	
Risk Management	Program	RI-01.1	Is your organization insured by a 3rd party for losses?	AWS provides customer remuneration for losses they may incur due to outages in alignment with AWS's Service Level Agreement.
Risk Management		RI-01.2	Do your organization's service level agreements provide tenant remuneration for losses they may incur due to outages or losses experienced within your infrastructure?	

Risk Management	Assessments	RI-02.1	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?	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 aws.amazon.com/security) for additional details on AWS Risk Management Framework.
Risk Management		RI-02.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	
Risk Management	Mitigation / Acceptance	RI-03.1	Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?	In alignment with ISO 27001 standard, Annex A, domain 4.2, 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) for additional details on AWS Risk Management Framework
		RI-03.2	Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?	
Risk Management	Business / Policy Change Impacts	RI-04.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Updates to AWS security policies, procedures, standards and controls occur on an annual basis in alignment with the ISO 27001 standard. Refer to ISO 27001 Annex A, domain 5.1 for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
Risk Management	Third Party Access	RI-05.1	Do you provide multi-failure disaster recovery capability?	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 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11. 2 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
		RI-05.2	Do you monitor service continuity with upstream providers in the event of provider failure?	
		RI-05.3	Do you have more than one provider for each service you depend on?	
		RI-05.4	Do you provide access to operational redundancy and continuity summaries which include the services on which you depend?	
		RI-05.5	Do you provide the tenant the ability to declare a disaster?	
		RI-05.6	Do you provide a tenant triggered failover option?	

		RI-05.7	Do you share your business continuity and redundancy plans with your tenants?	
Release Management	New Development / Acquisition	RM-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?	In alignment with ISO 27001 standards, AWS has in place procedures to manage new development of resources. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. In addition AWS SOC 1 Type 2 report provides further information.
Release Management	Production Changes	RM-02.1	Do you provide tenants with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?	AWS SOC 1 Type 2 report provides an overview of the controls in place to manage change Management in the AWS environment. In addition, refer to ISO 27001 standard, Annex A, domain 12.5 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Release Management	Quality Testing	RM-03.1	Do you provide your tenants with documentation which describes your quality assurance process?	AWS incorporates standards of quality as part of the system development lifecycle (SDLC) processes which are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 10.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Release Management	Outsourced Development	RM-04.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	AWS does not generally outsource development of software. AWS incorporates standards of quality as part of the system development lifecycle (SDLC) processes which are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 10.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Release Management		RM-04.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	
Release Management	Unauthorized Software Installations	RM-05.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	AWS's program, processes and procedures for managing malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC 1 Type 2 report provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 10.4 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Resiliency	Management Program	RS-01.1	Are Policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event and properly communicated to tenants?	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 14.1 and AWS SOC 1 report for further details on AWS and business continuity.
Resiliency	Impact Analysis	RS-02.1	Do you provide tenants with ongoing visibility and reporting into your operational Service Level Agreement (SLA) performance?	AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com.
Resiliency		RS-02.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	
Resiliency		RS-02.3	Do you provide customers with ongoing visibility and reporting into your SLA performance?	
Resiliency	Business Continuity Planning	RS-03.1	Do you provide tenants with geographically resilient hosting options?	Data centers are built in clusters in various global regions. 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. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security
Resiliency		RS-03.2	Do you provide tenants with infrastructure service failover capability to other providers?	
Resiliency	Business Continuity Testing	RS-04.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	AWS Business Continuity Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 14.1 and AWS SOC 1 report for further details on AWS and business continuity.
Resiliency	Environmental Risks	RS-05.1	Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?	AWS data centers incorporate physical protection against environmental risks. AWS's 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 9.1 and the AWS SOC 1 Type 2 report for additional information.

Resiliency	Equipment Location	RS-06.1	Are any of your datacenters located in places which have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	AWS data centers incorporate physical protection against environmental risks. AWS services provide customers the flexibility to store data within multiple geographical regions as well as across multiple Availability zones. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Refer to ISO 27001 standard, Annex A domain 9.1 and the AWS SOC 1 Type 2 report for additional information.
Resiliency	Equipment Power Failures	RS-07.1	Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	AWS equipment is protected from 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 1 Type 2 report provides additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities. In addition, refer to the AWS Overview of Security Processes Whitepaper - available at http://aws.amazon.com/security.
Resiliency	Power / Telecommunications	RS-08.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	AWS customers designate in which physical region their data and 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. AWS SOC 1 Type 2 report provides additional details. Customers can also choose their network path to AWS facilities, including over dedicated, private networks where the customer controls the traffic routing.
Resiliency		RS-08.2	Can Tenants define how their data is transported and through which legal jurisdiction?	
Security Architecture	Customer Access Requirements	SA-01.1	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?	AWS customers retain responsibility to ensure their usage of AWS is within compliance of applicable laws and regulations. AWS communicates its security and control environment to customers through industry certifications and third party attestations, white papers (available at http://aws.amazon.com/security) and providing certifications, reports and other relevant documentation directly to AWS customers. Refer to ISO 27001 standard, Annex A, domain 6.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Security Architecture	User ID Credentials	SA-02.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	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

Security Architecture		SA-02.2	Do you use open standards to delegate authentication capabilities to your tenants?	customer can utilize. Refer to the AWS website for additional details - http://aws.amazon.com/mfa.
Security Architecture		SA-02.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	
Security Architecture		SA-02.4	Do you have a Policy Enforcement Point capability (ex. XACML) to enforce regional legal and policy constraints on user access?	
Security Architecture		SA-02.5	Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a tenant)?	
Security Architecture		SA-02.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc..) for user access?	
Security Architecture		SA-02.7	Do you allow tenants to use third party identity assurance services?	
Security Architecture	Data Security / Integrity	SA-03.1	Is your Data Security Architecture designed using an industry standard? (ex. CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP CAESARS)	AWS Data Security Architecture was designed to incorporate industry leading practices. Refer to ISO 27001 standard, Annex A, domain 10.8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Security Architecture	Application Security	SA-04.1	Do you utilize industry standards (Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build-in security for your Systems/Software Development Lifecycle (SDLC)?	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. Refer to the AWS Overview of Security Processes for further details. In addition, refer to ISO 27001 standard, Annex A, domain 12.5 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Security Architecture		SA-04.2	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?	
Security Architecture		SA-04.3	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	

Security Architecture	Data Integrity	SA-05.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	AWS data integrity controls as described in AWS SOC 1 Type 2 report provides reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing. In addition, refer to ISO 27001 standard, Annex A, domain 12.2 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Security Architecture	Production / Nonproduction Environments	SA-06.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	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/.
Security Architecture		SA-06.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	
Security Architecture	Remote User Multifactor Authentication	SA-07.1	Is multi-factor authentication required for all remote user access?	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.
Security Architecture	Network Security	SA-08.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	The 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/.
Security Architecture	Segmentation	SA-09.1	Are system and network environments logically separated to ensure Business and customer security requirements?	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 11.4 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Security Architecture		SA-09.2	Are system and network environments logically separated to ensure compliance with legislative, regulatory, and contractual requirements?	
Security Architecture		SA-09.3	Are system and network environments logically separated to ensure separation of production and non-production environments?	
Security Architecture		SA-09.4	Are system and network environments logically separated to ensure protection and isolation of sensitive data?	
Security Architecture	Wireless Security	SA-10.1	Are policies and procedures established and mechanisms implemented to protect network environment parameter and configured to restrict unauthorized traffic?	Policies, procedures and mechanisms to protect AWS network environment are in place. AWS SOC 1 Type 2 report provides additional details. In addition refer to ISO 27001 standard, Annex A,

Security Architecture		SA-10.2	Are policies and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.)	domain 10.6 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Security Architecture		SA-10.3	Are policies and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	
Security Architecture	Shared Networks	SA-11.1	Is access to systems with shared network infrastructure restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations?	Access is strictly restricted to critical resources including services, hosts, and network devices and must be explicitly approved in Amazon's proprietary permission management system. AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS. In addition, refer to ISO 27001 standard, Annex A, domain 11. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Security Architecture	Clock Synchronization	SA-12.1	Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?	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.
Security Architecture	Equipment Identification	SA-13.1	Is automated equipment identification used as a method of connection authentication to validate connection authentication integrity based on known equipment location?	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.
Security Architecture	Audit Logging / Intrusion Detection	SA-14.1	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?	AWS Incident response program (detection, investigation and response to incidents) have been developed in alignment with ISO 27001 standard. AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS. The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details.
Security Architecture		SA-14.2	Is Physical and logical user access to audit logs restricted to authorized personnel?	
Security Architecture		SA-14.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	

Security Architecture	Mobile Code	SA-15.1	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?	AWS allows customers to manage client and mobile applications to their own requirements.
Security Architecture		SA-15.2	Is all unauthorized mobile code prevented from executing?	

APPENDIX B: AWS ALIGNMENT WITH MOTION PICTURE OF AMERICA ASSOCIATION (MPAA) CONTENT SECURITY MODEL.

The Motion Picture of America Association (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content (http://www.fightfilmtheft.org/facility-security-program.html). Media companies use these best practices as a way to assess risk and audit security of their content and infrastructure.

See below for the AWS alignment with Motion Picture of America Association (MPAA) Content Security Model.

Security Topic	Reference	MPAA Security Best Practice	AWS alignment with MPAA Best Practice
Executive Security Awareness/Oversight	MS-1.0	Ensure executive management / owner(s) oversight of the Information Security function by requiring periodic updates of the information security program and risk assessment results	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 established policies. Refer to AWS Risk & Compliance whitepaper for additional details - available at http://aws.amazon.com/security.
Executive Security Awareness/Oversight	MS-1.1	Train and engage executive management / owner(s) on the business' responsibilities to protect content	
Risk Management	MS-2.0	Develop a formal security risk assessment process focused on content workflows and sensitive assets in order to identify and prioritize risks of content theft and leakage that are relevant to the facility	Customers retain ownership of their data and are responsible for assessing and managing risk associated with the workflows of their data to meet their Compliance needs. AWS treats all Customer data and associated assets as Highly Confidential. 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 for further information available at http://aws.amazon.com/security.The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS.
Risk Management	MS-2.1	Identify high-security content based on client instruction	
Risk Management	MS-2.2	Perform a security risk assessment annually, update the risk assessment when key workflows change, and document and act upon identified risks	
Security Organization	MS-3.0	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection	AWS has an established information security organization managed by the AWS Security team and is led by the AWS Chief Information Security Officer (CISO). Refer to AWS Risk and Compliance Whitepaper for further information available at http://aws.amazon.com/security. In addition, the AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS.
Budgeting	MS-4.0	Document and budget for security initiatives, upgrades, and maintenance.	The role of the AWS Information Security and Compliance organization is to develop action plans, schedules and identify security initiatives intended to enhance AWS Information Security Program. The role of AWS CISO is to approve action plans, schedules, budgets and other associated management communications to support the continued efforts to enhance AWS Security efforts. Refer to the AWS Overview of Security Processes whitepaper for

			further information, available at http://aws.amazon.com/security.
Policies and Procedures	MS-5.0	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum: • Human resources policies • Acceptable use (e.g., social networking, Internet, phone, etc.) • Asset classification • Asset handling policies • Digital recording devices (e.g., smart phones, digital cameras, camcorders) • Exception policy • Password controls (e.g., password minimum length, screensavers) • Prohibition of client asset removal from the facility • System change management • Whistleblower policy	Customers retain responsibility of their data and development of associated policies and procedures to manage content security. As it pertains to AWS Information Assets, policies and procedures have been established by AWS Information Security based upon the COBIT framework, ISO 27001 standards and the PCI DSS requirements. 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 has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper for further information available at http://aws.amazon.com/security
Policies and Procedures	MS-5.1	Review and update security policies and procedures at least annually	
Policies and Procedures	MS-5.2	Require a sign-off from all company personnel (e.g., employees, temporary workers, interns) and third party workers (e.g., contractors, freelancers, temp agencies) for all policies, procedures, and/or client requirements and any updates	
Incident Response	MS-6.0	Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported	Customers retain control of their own guest operating systems, software and applications and are responsible for developing an incident response plan to meet their organizational requirements. AWS's incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS. The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details.
Incident Response	MS-6.1	Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents	
Incident Response	MS-6.2	Establish a security incident reporting process for individuals to report detected incidents to the security incident response team	
Incident Response	MS-6.3	Communicate incidents to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client assets), and conduct a post-mortem meeting with management and client	

Workflow	MS-7.0	Document a workflow that includes the tracking of content and authorization checkpoints throughout each process; include the following processes for both physical and digital content: • Delivery • Ingest • Movement • Storage • Return to originator • Removal from the site • Destruction	Customers retain control of their own guest operating systems, software, applications and data and are responsible for documenting workflow of content to meet their risk and compliance requirements. 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. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Workflow	MS-7.1	Identify, implement, and assess the effectiveness of key controls to prevent, detect, and correct risks related to the content workflow	
Segregation of Duties	MS-8.0	Segregate duties within the content workflow	Customers retain control of their own guest operating systems, software, applications and data and are responsible for applying segregation of duties within their environment. AWS aligns with ISO 27001 standard for managing segregation of duties. Refer to ISO 27001 standard, Annex A, domain 10.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Segregation of Duties	MS-8.1	Implement and document compensating controls where segregation is not practical	
Background Checks	MS-9.0	Perform background screening checks on all company personnel and third party workers	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. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Confidentiality Agreements	MS-10.0	Require all company personnel and third party workers to sign a confidentiality agreement (e.g., non-disclosure) upon hire and annually thereafter, that includes requirements for handling and protecting content	Amazon Legal Counsel manages and periodically revises the Amazon Non-Disclosure Agreement (NDA) to reflect AWS business needs. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Confidentiality Agreements	MS-10.1	Require all company personnel and third party workers to return all content and client information in their possession upon termination of their employment or contract	

Disciplinary Measures	MS-11.0	Define and communicate disciplinary measures for violations of facility policies to all company personnel and third party workers	AWS provides security policy and provides security training to employees to educate them as to their role and responsibilities concerning information security. Employees who violate Amazon standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed. Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. Refer to ISO 27001 Annex A, domain 8.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Content Security and Piracy Awareness	MS-12.0	Develop and regularly update a security awareness program and train company personnel and third party workers upon hire and annually thereafter, addressing the following areas at a minimum: • IT security policies and procedures • Content/asset security and handling • Security incident reporting and escalation • Disciplinary measures	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 has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper for further information available at http://aws.amazon.com/security.
Third Party Use and Screening	MS-13.0	Require all third party workers who handle content to sign confidentiality agreements (e.g., non-disclosure) upon engagement	Customers retain control of their production areas and data and are responsible for developing third party policies to meet their risk and compliance needs. Amazon Legal Counsel manages Amazon Non-Disclosure Agreement (NDA) to reflect AWS business needs. Non-Disclosure Agreements are provided to third party Contractors and Vendors and employees that work with AWS. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Third Party Use and Screening	MS-13.1	Include security requirements in third party contracts	
Third Party Use and Screening	MS-13.2	Implement a process to reclaim assets and remind third party workers of confidentiality agreements and contractual security requirements when terminating relationships	
Third Party Use and Screening	MS-13.3	Require third party workers to be bonded and insured where appropriate (e.g., courier service)	
Third Party Use and Screening	MS-13.4	Restrict third party access to content/production areas unless required for their job function	
Third Party Use and Screening	MS-13.5	Require third party companies to notify clients if they are on-boarding additional third party companies to handle content	
Entry/Exit Points	PS-1.0	Lock all entry/exit points at all times if the facility does not have a segregated access-controlled area beyond reception	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 datacenter floors. Refer to AWS Overview of Security Processes Whitepaper for further information available at http://aws.amazon.com/security.
Entry/Exit Points	PS-1.1	Control access to production areas by segregating the content/production area from other facility areas (e.g., administrative offices)	

Entry/Exit Points	PS-1.2	Require rooms used for screening purposes to be access-controlled (e.g., projection booths)	In addition, the AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS.
Visitor Entry/Exit	PS-2.0	Maintain a detailed visitors' log which includes the following: • Name • Company • Time in/time out • Person/people visited • Signature of visitor • Badge number assigned	AWS provides data center physical access and information to approved employees and contractors who have a legitimate business need for such privileges. All visitors are required to present identification and are signed in and escorted by authorized staff. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper for further information available at http://aws.amazon.com/security
Visitor Entry/Exit	PS-2.1	Assign an identification badge or sticker, which must be visible at all times, to each visitor and collect badges upon exit	
Visitor Entry/Exit	PS-2.2	Do not provide visitors with electronic access to content/production areas	
Visitor Entry/Exit	PS-2.3	Require visitors to be escorted by authorized employees while on-site, or in content/production areas at a minimum	
Identification	PS-3.0	Provide company personnel and long-term third party workers (e.g., janitorial) with photo identification that is validated and required to be visible at all times	AWS provides personnel with approved long term data center access an electronic access card with photographic identification. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper for further information available at http://aws.amazon.com/security
Perimeter Security	PS-4.0	Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's risk assessment	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 1 Type 2 report and AWS SOC 2 Type 2 report provide additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper for further information available at http://aws.amazon.com/security
Emergency Protocol	PS-5.0	Install a power backup system (e.g., Uninterruptible Power Supply or "UPS") to support security installations (e.g., CCTV system, alarm system, electronic access system) and critical production systems for at least 15 minutes to allow enough time for the facility to be secured upon an emergency, incident, or power outage	AWS equipment is protected from 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. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provide additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities. In addition, refer to the AWS Overview of Security Processes Whitepaper - available at http://aws.amazon.com/security.
Emergency Protocol	PS-5.1	Test and conduct maintenance for the power backup system at least annually	
Emergency Protocol	PS-5.2	Configure electronic access systems, when implemented at the facility, as fail-secure in case of a power outage	
Alarms	PS-6.0	Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), loading docks, fire escapes, and	Physical security controls include security staff, video surveillance and intrusion detection systems. Alarms are escalated to and monitored by the AWS physical security staff. Authorized staff must pass two-factor authentication a minimum of two times to

		restricted areas (e.g., vault, server/machine room)	access datacenter floors. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper and the AWS Overview of Security Processes Whitepaper for further information available at http://aws.amazon.com/security
Alarms	PS-6.1	Configure alarms to provide escalation notifications directly to the personnel in charge of security and/or be monitored by a central security group or third party	
Alarms	PS-6.2	Assign unique arm and disarm codes to each person that requires access to the alarm system and restrict access to all other personnel	
Alarms	PS-6.3	Review the list of users who can arm and disarm alarm systems annually	
Alarms	PS-6.4	Test the alarm system every 6 months	
Alarms	PS-6.5	Install and effectively position motion detectors in restricted areas (e.g., vault, server/machine room) and configure them to alert the appropriate security personnel and/or third-party	
Alarms	PS-6.6	Install door prop alarms for content/production areas to notify when sensitive entry/exit points are open for longer than a pre-determined period of time (e.g., 60 seconds)	
Authorization	PS-7.0	Document and implement a process to manage facility access and keep records of any changes to access rights	AWS has established formal policies and procedures to delineate the minimum standards for physical access to AWS data centers. Cardholder access to data centers is reviewed quarterly. Cardholders marked for removal have their access revokes as part of the quarterly review. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper and the AWS Overview of Security Processes Whitepaper for further information available at http://aws.amazon.com/security
Authorization	PS-7.1	Review access to restricted areas (e.g., vault, server/machine room) quarterly and when the roles or employment status of company personnel and/or third party workers are changed	
Electronic Access	PS-8.0	Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed	Physical access is controlled both at the perimeter and at building ingress points by 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. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper and the AWS Overview of Security Processes Whitepaper for further information available at http://aws.amazon.com/security
Electronic Access	PS-8.1	Restrict electronic access system administration to appropriate personnel	
Electronic Access	PS-8.2	Store blank card stock in a locked cabinet and ensure keycards remain disabled prior to being assigned to personnel	
Electronic Access	PS-8.3	Disable lost keycards in the system before issuing a new keycard	
Electronic Access	PS-8.4	Remove physical locks for restricted areas (e.g., vault, server/machine room) where an electronic access system is implemented	

Electronic Access	PS-8.5	Issue third party access cards with a set expiration date (e.g. 90 days) based on an approved timeframe	
Keys	PS-9.0	Limit the distribution of master keys to authorized personnel only (e.g., owner, facilities management)	Physical security processes and procedures, including procedures for managing facility Master keys are owned, managed and executed by AWS physical security staff. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper and the AWS Overview of Security Processes Whitepaper for further information available at http://aws.amazon.com/security
Keys	PS-9.1	Implement a check-in/check-out process to track and monitor the distribution of master keys	
Keys	PS-9.2	Use keys that can only be copied by a specific locksmith for exterior entry/exit points	
Keys	PS-9.3	Inventory master keys and keys to restricted areas, including facility entry/exit points, quarterly	
Cameras	PS-10.0	Install a CCTV system that records all facility entry/exit points and restricted areas	Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems and other electronic means. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper and the AWS Overview of Security Processes Whitepaper for further information available at http://aws.amazon.com/security.
Cameras	PS-10.1	Implement controls to ensure that camera footage is clear and visible in all lighting conditions	
Cameras	PS-10.2	Restrict physical and logical access to the CCTV console and to CCTV equipment (e.g., DVRs) to personnel responsible for administering/monitoring the system	
Cameras	PS-10.3	Review camera positioning, image quality, frame rate, and adequate retention of surveillance footage weekly	
Cameras	PS-10.4	Ensure that camera footage includes an accurate date and time-stamp	
Logging and Monitoring	PS-11.0	Log and review electronic access to restricted areas for suspicious events	Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems and other electronic means. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper and the AWS Overview of Security Processes Whitepaper for further information available at http://aws.amazon.com/security
Logging and Monitoring	PS-11.1	Investigate suspicious electronic access activities that are detected	
Logging and Monitoring	PS-11.2	Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken	
Logging and Monitoring	PS-11.3	Retain CCTV surveillance footage and electronic access logs for at least 90 days, or the maximum time allowed by law, in a secure location	
Searches	PS-12.0	Inform company personnel and third party workers upon hire that bags and packages are subject to random searches and include a provision addressing searches in the facility policies	AWS reserves the right to execute a search of bags and packages in the event of an issue.
Inventory Tracking	PS-13.0	Implement a content asset management system to provide detailed tracking of physical assets (i.e., client and newly created)	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to implement inventory tracking of their physical assets. 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.
Inventory Tracking	PS-13.1	Barcode client assets and created media (e.g., tapes, hard drives) upon receipt and store assets in the vault when not in use	

Inventory Tracking	PS-13.2	Retain asset movement transaction logs for at least 90 days	Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Inventory Tracking	PS-13.3	Review logs from content asset management system and investigate anomalies	
Inventory Tracking	PS-13.4	Use studio AKAs (“aliases”) when applicable in asset tracking systems and on any physical assets	
Inventory Counts	PS-14.0	Perform a quarterly inventory count of each client's pre-release project(s), reconcile against asset management records, and immediately communicate variances to clients	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to implement inventory tracking and monitoring of their physical assets. Internally, 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. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Inventory Counts	PS-14.1	Segregate duties between the vault staff and individuals who are responsible for performing inventory counts	
Inventory Counts	PS-14.2	Implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault and not checked back in	
Blank Media/ Raw Stock Tracking	PS-15.0	Tag (e.g., barcode, assign unique identifier) blank stock / raw stock per unit when received	AWS customers retain control and ownership of their data and media assets. It is the customer's responsibility to manage security of media stock.
Blank Media/ Raw Stock Tracking	PS-15.1	Store blank media / raw stock in a secured location	
Client Assets	PS-16.0	Restrict access to finished client assets to personnel responsible for tracking and managing assets	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to restrict access to their physical assets. Internally, 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. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Client Assets	PS-16.1	Store client assets in a restricted and secure area (e.g., vault, safe)	

Production Systems	PS-17.0	Restrict access to production systems to appropriate personnel only	Customers retain control of their own guest operating systems, software and applications and are responsible for implementing appropriate restrictions to their production environment. Administrators with a business need to access the management plane are required to use multifactor authentication 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 of the cloud. 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. The AWS SOC 1 Type 2 report and AWS SOC 2 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to AWS Risk and Compliance Whitepaper and the AWS Overview of Security Processes Whitepaper for further information available at http://aws.amazon.com/security
Disposals	PS-18.0	Require that rejected, damaged, and obsolete stock are erased, degaussed, shredded, or physically destroyed before disposal (e.g., DVD shredding, hard drive destruction) and update asset management records to reflect destruction	Customers retain responsibility to dispose of physical media assets per their own requirements. Internally, when an AWS 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 DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
Disposals	PS-18.1	Follow the Department of Defense (DoD) clearing and sanitizing standards for digital shredding and wiping	
Disposals	PS-18.2	Store elements targeted for recycling/destruction in a secure location/container to prevent the copying and reuse of assets prior to disposal	
Disposals	PS-18.3	Maintain a log of asset disposal for at least 12 months	
Disposals	PS-18.4	Require third-party companies who handle destruction of content to provide a certificate of destruction for each completed job	
Disposals	PS-18.5	Destroy check discs immediately after use	
Shipping	PS-19.0	Require the facility to file a valid work / shipping order to authorize asset shipments out of the facility	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage shipping and receiving of their physical assets. 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. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Shipping	PS-19.1	Track and log asset shipping details; at a minimum, include the following: • Time of shipment • Sender name and signature • Recipient name • Address of destination • Tracking number from courier • Reference to the corresponding work order	

Shipping	PS-19.2	Validate assets leaving the facility against a valid work/shipping order	
Shipping	PS-19.3	Secure assets that are waiting to be picked up	
Shipping	PS-19.4	Prohibit couriers and delivery personnel from entering content/production areas of the facility	
Receiving	PS-20.0	Inspect delivered content upon receipt and compare to shipping documents (e.g., packing slip, manifest log)	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage shipping and receiving of their physical assets. Internally, 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. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Receiving	PS-20.1	Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries	
Receiving	PS-20.2	Perform the following actions immediately: • Tag (e.g., barcode, assign unique identifier) received assets, • Input the asset into the asset management system • Move the asset to the restricted area (e.g., vault, safe)	
Receiving	PS-20.3	Implement a secure method (e.g., secure drop box) for receiving overnight deliveries	
Labeling	PS-21.0	Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage shipping and receiving procedures for their physical assets. 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. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Labeling	PS-21.1	Include a return address that excludes the client or company name on all outgoing packages	
Packaging	PS-22.0	Ship all assets in closed/sealed containers, and use locked containers depending on asset value	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage shipping and receiving of their physical assets. 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. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Packaging	PS-22.1	Implement at least one of the following controls: • Tamper-evident tape • Tamper-evident packaging • Tamper-evident seals in the form of holograms • Secure containers (e.g., Pelican case with a combination lock)	

Transport Vehicles	PS-23.0	Lock automobiles and trucks at all times, and do not place packages in visible auto/truck areas	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage shipping and receiving of their physical assets. Internally, 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. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
WAN	DS-1.0	Segment WAN(s) by using stateful inspection firewalls with Access Control Lists that prevent unauthorized access to any internal network	Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny-all mode and Amazon EC2 customers must explicitly open the ports needed to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block). Amazon RDS database instance access is controlled by the customer via Database Security Groups which are similar to Amazon EC2 Security Groups, but are not interchangeable. Database Security Groups default to a "deny all" access mode and customers must specifically authorize network ingress. Amazon ElastiCache allows customers to control access to Cache Clusters using Cache Security Groups. A Cache Security Group acts like a firewall, controlling network access to a Cache Cluster. AWS customers retain responsibility to manage their firewall settings and network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with ISO 27001 standards. In addition, firewall devices are configured to restrict access to Amazon's corporate and production networks. The configurations of these firewall policies are maintained via an automatic push from a parent server every 24 hours. Refer to ISO 27001 standard, Annex A. domain 11.4 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
WAN	DS-1.1	Develop a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the business every 6 months	
WAN	DS-1.2	Deny all protocols by default and enable only specific permitted secure protocols on the WAN	
WAN	DS-1.3	Place externally accessible servers (e.g., secure FTP server, web servers) within the DMZ	
WAN	DS-1.4	Implement a process to patch network infrastructure devices (e.g., firewalls, routers, switches, etc.) regularly	
WAN	DS-1.5	Harden network infrastructure devices based on security configuration standards	
WAN	DS-1.6	Do not allow remote access to WAN network infrastructure devices (e.g., firewall, router) that control access to content	
WAN	DS-1.7	Secure backups of network infrastructure devices to a centrally secured server on the internal network	
WAN	DS-1.8	Perform an annual vulnerability scan on hosts that are externally accessible and remediate issues	
WAN	DS-1.9	Ensure that after opening a fiber connection through a telecom service provider, the connection is terminated after the session ends	
WAN	DS-1.10	Allow only authorized personnel to request the establishment of a connection with the telecom service provider	
Internet	DS-2.0	Prohibit Internet access on systems (desktops/ servers) that process or store digital content	AWS customers retain control and ownership of their operating systems, software, applications, desktops, e-mail and web filtering.

Internet	DS-2.1	Implement e-mail filtering software or appliances that block the following from non-content/production networks: • Potential phishing e-mails • Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.) • File size restrictions limited to 10 MB	AWS's program, processes and procedures to managing e-mail filtering, antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC 1 Type 2 report provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 10.4 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Internet	DS-2.2	Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites	
LAN	DS-3.0	Isolate the content/production network from non-production networks (e.g., office network, DMZ, etc.) by means of physical or logical network segmentation	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 11.4 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
LAN	DS-3.1	Restrict access to the content/production systems to authorized personnel	
LAN	DS-3.2	Restrict remote access to the content/production network to only approved personnel who require access to perform their job responsibilities	
LAN	DS-3.3	Disable all unused switch ports on the content/production network to prevent packet sniffing by unauthorized devices	
LAN	DS-3.4	Restrict the use of non-switched devices such as hubs and repeaters on the content/production network	
LAN	DS-3.5	Prohibit dual-homed networking (network bridging) on computer systems within the content/production network	
LAN	DS-3.6	Implement a network-based intrusion detection or prevention system on the content/production network	
Wireless	DS-4.0	Prohibit wireless networking and the use of wireless devices on the production/content network	Customers retain responsibility for managing, monitoring and configuring their wireless security.

Wireless	DS-4.1	Configure wireless networks on the non-production/content network with strong security controls: • Disable SSID broadcasting • Disable WEP • Enable AES encryption • Enable IEEE 802.1X or IEEE 802.11i where the option is available • Use RADIUS for authentication where the option is available Implement the following controls if pre-shared keys must be used: • Configure WPA2 with CCMP (AES) encryption • Set a complex passphrase (See DS-8.1 for passphrase complexity recommendations) • Change the passphrase periodically and when key company personnel terminate their employment • Enable MAC address filtering	Policies, procedures and mechanisms to protect Amazon network environment and wireless security are in place. AWS SOC 1 Type 2 report and SOC 2 Type 2 report provides additional details. In addition refer to ISO 27001 standard, Annex A, domain 10.6 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Wireless	DS-4.2	Implement a process to scan for rogue wireless access points annually	
Wireless	DS-4.3	Reduce the transmission power of the wireless access points to provide wireless networking to a limited coverage area	
I/O Device Security	DS-5.0	Designate specific systems to be used for content input/output (I/O)	Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt data and implement policies to manage input/output devices. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. AWS key management procedures are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 15.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
I/O Device Security	DS-5.1	Block input/output (I/O) devices (e.g., USB, FireWire, e-SATA, SCSI, etc.) on all systems that handle or store content, with the exception of systems used for content I/O	
I/O Device Security	DS-5.2	Restrict the installation and/or use of media burners (e.g., DVD, Blu-ray, CD burners) and other devices with output capabilities to specific I/O systems used for outputting content to physical media	
I/O Device Security	DS-5.3	Implement AES 128-bit encryption on hard drives and USB flash memory used to transport content	
I/O Device Security	DS-5.4	Prohibit the use of digital recording devices (e.g., smart phones, digital cameras, camcorders) in areas where sensitive content is accessible electronically	
System Security	DS-6.0	Install anti-virus software on all workstations and servers	Customers are responsible for the development, content, operation, maintenance, and use of their content. Customers retain control of their own guest operating systems, software and applications and are responsible for developing associated policies, procedures and guidelines to manage and operate their environment. Customers are also responsible for performing
System Security	DS-6.1	Update anti-virus definitions daily	
System Security	DS-6.2	Scan file-based content for viruses prior to ingest onto the content/production network	

System Security	DS-6.3	Document and implement a strategy for performing virus scans such as: • Enable regular full system virus scanning on all workstations • Enable full system virus scans for servers, where applicable (e.g., non-SAN systems)	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's own maintenance and system patching generally do not impact customers. Refer to AWS Overview of Security Processes Whitepaper for further information - available at http://aws.amazon.com/security. Refer to ISO 27001 standard, Annex A, domain 12.5 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Internally, AWS's program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC 1 Type 2 report provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 10.4 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
System Security	DS-6.4	Implement a patch management process to regularly update patches (e.g., system, database, application, network devices) that remediate security vulnerabilities	
System Security	DS-6.5	Prohibit users from being Administrators on their own workstations	
System Security	DS-6.6	Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended	
System Security	DS-6.7	Install remote-kill software on all portable computing devices that handle content to allow remote wiping of hard drives and other storage devices	
System Security	DS-6.8	Restrict software installation privileges to system administrators	
System Security	DS-6.9	Require that legitimate licenses are used for all software and other proprietary software assets	
System Security	DS-6.10	Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers) that are set up internally	
System Security	DS-6.11	Unnecessary services and applications should be uninstalled from content transfer servers	
Account Management	DS-7.0	Establish and implement an account management process for administrator, user, and service accounts for all information systems and applications that handle content	Customers retain control of their own guest operating systems, software and applications and are responsible for implementing appropriate account management processes. Internally, in alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. Administrators with a business need to access the management plane are required to use multifactor authentication 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 of the cloud. 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 SOC 1 Type 2 report SOC 2 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security.
Account Management	DS-7.1	Maintain traceable evidence of the account management activities (e.g., approval e-mails, change request forms)	
Account Management	DS-7.2	Assign unique credentials on a need-to-know basis using the principles of least privilege	
Account Management	DS-7.3	Restrict the use of service accounts to only applications that require them	
Account Management	DS-7.4	Rename the default administrator accounts and limit the use of these accounts to special situations that require these credentials (e.g., operating system updates, patch installations, software updates)	

Account Management	DS-7.5	Segregate duties to ensure that individuals responsible for assigning access to information systems are not themselves end users of those systems (i.e., personnel should not be able to assign access to themselves)	
Account Management	DS-7.6	Monitor and audit administrator and service account activities	
Account Management	DS-7.7	Implement a process to review user access for all information systems that handle content and remove any user accounts that no longer require access quarterly	
Account Management	DS-7.8	Review user access to content on a per-project basis	
Account Management	DS-7.9	Disable or remove local accounts on systems that handle content	
Authentication	DS-8.0	Enforce the use of unique usernames and passwords to access information systems	AWS Identity and Access Management (AWS IAM) enables a customer to create multiple users and manage the permissions for each of these users within their AWS Account. A user is an identity (within a customer AWS Account) with unique security credentials that can be used to access AWS Services. AWS IAM eliminates the need to share passwords or access keys, and makes it easy to enable or disable a user's access as appropriate. 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. Internally, AWS User Account Management is in alignment with ISO 27001 standard. AWS SOC 1 Type 2 report SOC 2 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security.
Authentication	DS-8.1	Enforce a strong password policy for gaining access to information systems	
Authentication	DS-8.2	Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the network	
Authentication	DS-8.3	Implement password-protected screensavers for servers and workstations	
Logging and Monitoring	DS-9.0	Implement real-time logging and reporting systems to record and report security events; gather the following information at a minimum: • When (time stamp) • Where (source) • Who (user name) • What (content)	Customers retain control of their own guest operating systems, software and applications and are responsible for implementing appropriate log management policies to meet their operational, risk and compliance needs. In alignment with ISO 27001 standards, AWS has established formal policies, procedures to manage logging and incident response. AWS SOC 1 Type 2 and SOC 2 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security.
Logging and Monitoring	DS-9.1	Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents	
Logging and Monitoring	DS-9.2	Investigate any unusual activity reported by the logging and reporting systems	
Logging and Monitoring	DS-9.3	Review logs weekly	
Logging and Monitoring	DS-9.4	Enable logging on content transfers and include the following information at a minimum: • Username • Timestamp • File name • Source IP address • Destination IP address • Event (e.g., download, view)	

Logging and Monitoring	DS-9.5	Retain logs for at least 6 months	
Logging and Monitoring	DS-9.6	Restrict log access to appropriate personnel	
Logging and Monitoring	DS-9.7	Send automatic notifications to the production coordinator(s) upon outbound content transmission	
Security Techniques	DS-10.0	Ensure that security techniques (e.g., spoiling, invisible/visible watermarking) are available for use and are applied when instructed	Customers retain ownership of their data and the responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
Security Techniques	DS-10.1	Encrypt content on hard drives using AES 128-bit encryption by either: • File-based encryption: (i.e., encrypting the content itself) • Drive-based encryption: (i.e., encrypting the hard drive)	
Security Techniques	DS-10.2	Send decryption keys or passwords using an out-of-band communication protocol (i.e., not on the same storage media as the content itself)	
Transfer Tools	DS-11.0	Implement transfer tools that use access controls, a minimum of AES 128-bit encryption and strong authentication for content transfer sessions	Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
Transfer Tools	DS-11.1	Implement an exception process, where client prior approval must be obtained in writing, to address situations where encrypted transfer tools are not used	
Transfer Device Methodology	DS-12.0	Implement and use dedicated systems for content transfers	Customers retain control of their data, guest operating systems, software and applications and are responsible for implementing appropriate policies and procedures for managing their content and managing network segmentation and deletion of data.
Transfer Device Methodology	DS-12.1	Segment systems dedicated to transfer files from systems that store or process content and from the non-production network	
Transfer Device Methodology	DS-12.2	Place content transfer systems in a Demilitarized Zone (DMZ) and not in the production/content network	
Transfer Device Methodology	DS-12.3	Remove content from content transfer devices immediately after successful transmission/receipt	
Client Portal	DS-13.0	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users	Customers retain ownership of their guest operating systems, software and applications, and all associated business process, procedures and guidelines. 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's own maintenance and system patching generally do not impact customers. Refer to AWS Overview of Security Processes Whitepaper for
Client Portal	DS-13.1	Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely	
Client Portal	DS-13.2	Ensure users only have access to their own digital assets (i.e., client A must not have access to client B's content)	
Client Portal	DS-13.3	Place the web portal on a dedicated server in the DMZ and limit access to/from specific IPs and protocols	

Client Portal	DS-13.4	Use HTTPS and enforce use of a strong cipher suite (e.g.,SSLv3 or TLS v1) for the internal/external web portal	further information - available at http://aws.amazon.com/security.
Client Portal	DS-13.5	Do not use persistent cookies or cookies that store credentials in plaintext	
Client Portal	DS-13.6	Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable	
Client Portal	DS-13.7	Restrict client portal access to originate from a specific IP address or range	
Client Portal	DS-13.8	Test for web application vulnerabilities annually	
Client Portal	DS-13.9	Allow only authorized personnel to request the establishment of a connection with the telecom service provider	
Client Portal	DS-13.10	Prohibit transmission of content using e-mail (including webmail) from the non-production network, and manage exceptions using the exception policy	
Client Portal	DS-13.11	Review access to the client web portal at least quarterly	

APPENDIX C – GLOSSARY OF TERMS

Authentication: Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

Availability Zone: Amazon EC2 locations are composed of regions and Availability Zones. Availability Zones are distinct locations that are engineered to be insulated from failures in other Availability Zones and provide inexpensive, low latency network connectivity to other Availability Zones in the same region.

DSS: The Payment Card Industry Data Security Standard (DSS) is a worldwide information security standard assembled and managed by the Payment Card Industry Security Standards Council.

EBS: Amazon Elastic Block Store (EBS) provides block level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are off-instance storage that persists independently from the life of an instance.

FISMA: The Federal Information Security Management Act of 2002. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FIPS 140-2: The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information.

GLBA: The Gramm–Leach–Bliley Act (GLB or GLBA), also known as the Financial Services Modernization Act of 1999, sets forth requirements for financial institutions with regard to, among other things, the disclosure of nonpublic customer information and the protection of threats in security and data integrity.

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

Hypervisor: A hypervisor, also called Virtual Machine Monitor (VMM), is software/hardware platform virtualization software that allows multiple operating systems to run on a host computer concurrently.

IAM: AWS Identity and Access Management (IAM) enables a customer to create multiple Users and manage the permissions for each of these Users within their AWS Account.

ITAR: International Traffic in Arms Regulations (ITAR) is a set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML). Government agencies and contractors must comply with ITAR and restrict access to protected data.

ISAE 3402: The International Standards for Assurance Engagements No. 3402 (ISAE 3402) is the international standard on assurance engagements. It was put forth by the International Auditing and Assurance Standards Board (IAASB), a standard-setting board within the International Federation of Accountants (IFAC). ISAE 3402 is now the new globally recognized standard for assurance reporting on service organizations.

ISO 27001: ISO/IEC 27001 is an Information Security Management System (ISMS) standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be audited and certified compliant with the standard.

NIST: National Institute of Standards and Technology. This agency sets detailed security standards as needed by industry or government programs. Compliance with FISMA requires agencies to adhere to NIST standards.

Object: The fundamental entities stored in Amazon S3. Objects consist of object data and metadata. The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object. These include some default metadata such as the date last modified and standard HTTP metadata such as Content-Type. The developer can also specify custom metadata at the time the Object is stored.

PCI: Refers to the Payment Card Industry Security Standards Council, an independent council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard.

QSA: The Payment Card Industry (PCI) Qualified Security Assessor (QSA) designation is conferred by the PCI Security Standards Council to those individuals that meet specific qualification requirements and are authorized to perform PCI compliance assessments.

SAS 70: Statement on Auditing Standards No. 70: Service Organizations is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SAS 70 provides guidance to service auditors when assessing the internal controls of a service organization (such as AWS) and issuing a service auditor's report. SAS 70 also provides guidance to auditors of financial statements of an entity that uses one or more service organizations. The SAS 70 report has been replaced by the Service Organization Controls 1 report.

Service: Software or computing ability provided across a network (e.g., EC2, S3, VPC, etc.).

Service Level Agreement (SLA): A service level agreement is a part of a service contract where the level of service is formally defined. The SLA is used to refer to the contracted delivery time (of the service) or performance.

SOC 1: Service Organization Controls 1 (SOC 1) Type II report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report (commonly referred to as the SSAE 16 report), is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The international standard is referenced as the International Standards for Assurance Engagements No. 3402 (ISAE 3402).

SSAE 16: The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is an attestation standard published by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). The standard addresses engagements undertaken by a service auditor for reporting on controls at organizations that provide services to user entities, for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting (ICFR). SSAE 16 effectively replaces Statement on Auditing Standards No. 70 (SAS 70) for service auditor's reporting periods ending on or after June 15, 2011.

Virtual Instance: Once an AMI has been launched, the resulting running system is referred to as an instance. All instances based on the same AMI start out identical and any information on them is lost when the instances are terminated or fail.

Version History

January 2013 version
- Edits to certifications and third-party attestations summaries
- Addition of the AWS Alignment with MPAA Content Security Model (Appendix B)

November 2012 version
- Edits to content and updated certification scope
- Added reference to the SOC 2 and MPAA

July 2012 version
- Edits to content and updated certification scope
- Addition of the CSA Consensus Assessments Initiative Questionnaire (Appendix A)

January 2012 version
- Minor edits to content based on updated certification scope
- Minor grammatical edits

December 2011 version
- Change to Certifications and Third-party Attestation section to reflect SOC 1/SSAE 16, FISMA Moderate, International Traffic in Arms Regulations, and FIPS 140-2
- Addition of S3 Server Side Encryption
- Added additional cloud computing issue topics

May 2011 version
Initial release

Notices