Chapter 13
AWS Risk and Compliance

THE AWS CERTIFIED SOLUTIONS ARCHITECT ASSOCIATE EXAM OBJECTIVES COVERED IN THIS CHAPTER MAY INCLUDE, BUT ARE NOT LIMITED TO, THE FOLLOWING:

Domain 2.0: Implementation/Deployment

✓2.1 Identify the appropriate techniques and methods using Amazon EC2, Amazon Simple Storage Service (Amazon S3), AWS Elastic Beanstalk, AWS CloudFormation, AWS OpsWorks, Amazon Virtual Private Cloud (Amazon VPC), and AWS Identity and Access Management (IAM) to code and implement a cloud solution.

Content may include the following:

- Configure services to support compliance requirements in the cloud

Domain 3.0: Data Security

✓3.1 Recognize and implement secure practices for optimum cloud deployment and maintenance.

Content may include the following:

- Shared security responsibility model
- Security Architecture with AWS
- AWS platform compliance
- AWS security attributes
- Design patterns

Introduction

AWS and its customers share control over the IT environment, so both parties have responsibility for managing that 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 customer is responsible for configuring their IT environment in a secure and controlled manner for their purposes. While customers don't communicate their use and configurations to AWS, AWS does communicate with customers regarding its security and control environment, as relevant. AWS disseminates this information using three primary mechanisms. First, AWS works diligently to obtain industry certifications and independent third-party attestations. Second, AWS openly publishes information about its security and control practices in whitepapers and website content. Finally, AWS provides certificates, reports, and other documentation directly to its customers under Non-Disclosure Agreements (NDAs) as required.

Overview of Compliance in AWS

When customers move their production workloads to the AWS cloud, both parties become responsible for managing the IT environment. The customers are responsible for setting up their environment in a secure and controlled manner. The customers also need to maintain adequate governance over their entire IT control environment. This section describes the AWS shared responsibility model and gives advice for how to establish strong compliance.

Shared Responsibility Model

As mentioned in Chapter 12, “Security on AWS,” as customers migrate their IT environments to AWS, they create a model of shared responsibility between themselves and AWS. This shared responsibility model can help lessen a customer’s IT operational burden, as it is AWS responsibility to manage the components from the host operating system and virtualization layer down to the physical security of the data centers in which these services operate. The customer is responsible for the components from the guest operating system upward (including updates, security patches, and antivirus software). The customer is also responsible for any other application software, as well as the configuration of security groups, Virtual Private Clouds (VPCs), and so on.

While AWS manages the security of the cloud, security in the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems, and networks, no differently than they would for applications in an on-site data center. Figure 13.1 illustrates the demarcation between customer and AWS responsibilities.

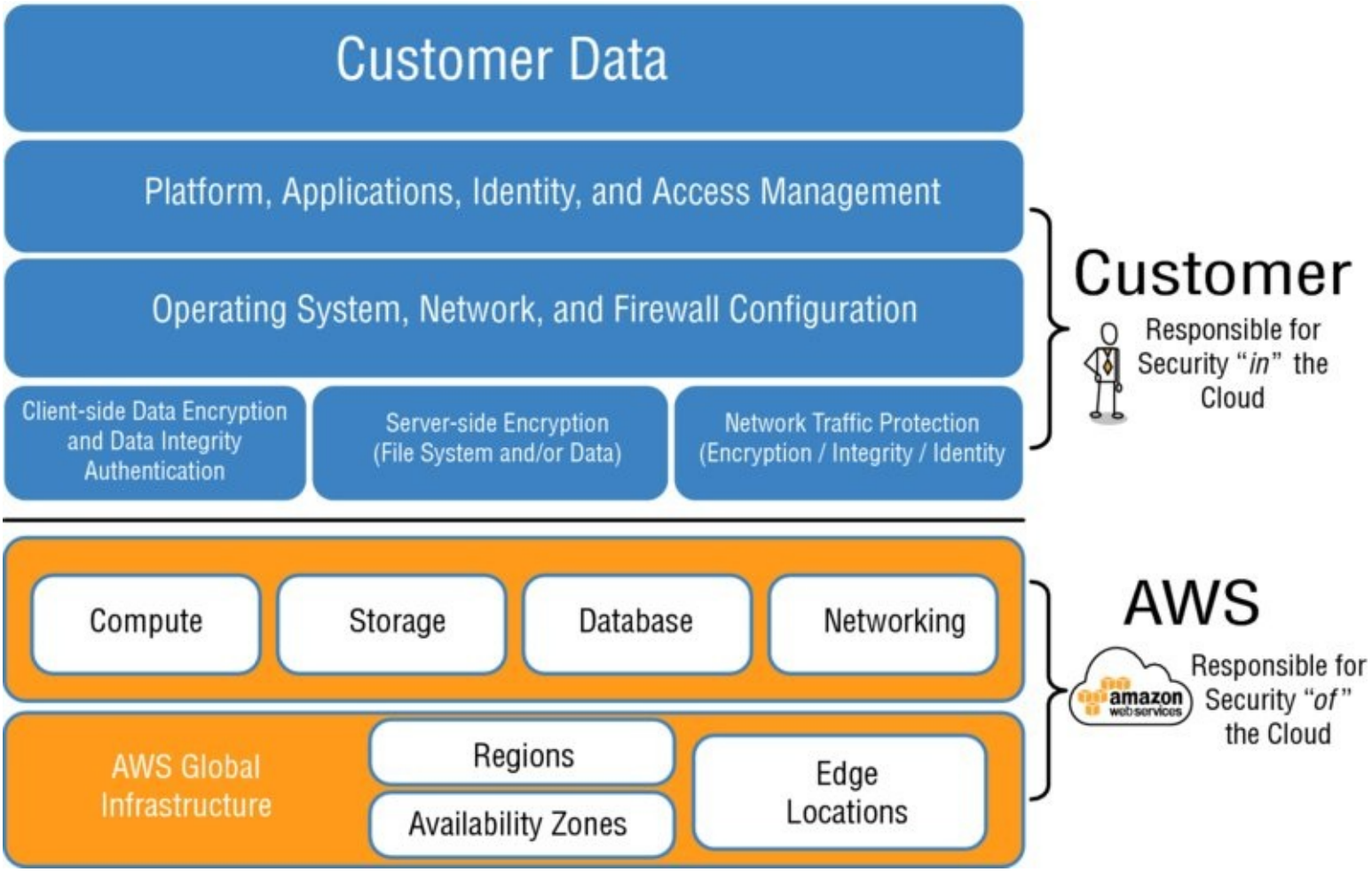

FIGURE 13.1 Shared responsibility model

Customers need to be aware of any applicable laws and regulations with which they have to comply, and then they must consider whether the services that they consume on AWS are compliant with these laws. In some cases, it may be necessary to enhance an existing platform on AWS with additional security measures (such as deploying a web application firewall, Intrusion Detection System [IDS], or Intrusion Prevention System [IPS], or using some form of encryption for data at rest).

This customer/AWS shared responsibility model is not just limited to security considerations, but it also extends to IT controls. For example, the management, operation, and verification of IT controls are shared between AWS and the customer. Before moving to the AWS Cloud, customers were responsible for managing all of the IT controls in their environments. AWS manages the controls for the physical infrastructure, thereby taking the undifferentiated heavy lifting from customers, allowing them to focus on managing the relevant IT controls. Because every customer is deployed differently in AWS, customers can shift management of certain IT controls to AWS. This change in management of IT controls results in a new, distributed control environment. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required.

Strong Compliance Governance

It is still the customers' responsibility to maintain adequate governance over the entire IT control environment, regardless of how their IT is deployed (whether it is on-premises, on the cloud, or part of a hybrid environment). By deploying to the AWS Cloud, customers have

options to apply different types of controls and various verification methods.

To achieve strong compliance and governance, customers may want to follow this basic methodology:

1. Take a holistic approach. Review the information available from AWS together with all other information to understand as much of the IT environment as they can. After this is complete, document all compliance requirements.
2. Design and implement control objectives to meet the organization's compliance requirements.
3. Identify and document controls owned by all third parties.
4. Verify that all control objectives are met and all key controls are designed and operating effectively.

By using this basic methodology, customers can gain a better understanding of their control environment. Ultimately, this will streamline the process and help separate any verification activities that need to be performed.

Evaluating and Integrating AWS Controls

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

Traditionally, the design and operating effectiveness of controls and control objectives are validated by internal and/or external auditors via process walkthroughs and evidence evaluation. Direct observation and 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 controls and control objectives. As a result, although a customer's key controls may be managed by AWS, the control environment can still be a unified framework in which all controls are accounted for and are verified as operating effectively. AWS third-party attestations and certifications not only provide a higher level of validation of the control environment, but may also relieve customers of the requirement to perform certain validation work themselves.

AWS IT Control Information

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

Specific Control Definition

AWS customers can 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 meet compliance requirements (for example, an 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 Type II report, formerly the *Statement on Auditing Standards (SAS) No. 70*, 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 that 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 effectively designed and operating for many compliance purposes, including Sarbanes-Oxley (SOX) Section 404 financial statement audits. Leveraging SOC 1 Type II reports is also generally permitted by other external certifying bodies. For example, *International Organization for Standardization (ISO) 27001* auditors may request a SOC 1 Type II report in order to complete their evaluations for customers.

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 *ISO 27001* certification, AWS complies with a broad, comprehensive security standard and follows best practices in maintaining a secure environment. With the *Payment Card Industry (PCI) Data Security Standard (DSS)* certification, AWS complies with a set of controls important to companies that handle credit card information. AWS compliance with *Federal Information Security Management Act (FISMA)* standards means that AWS complies with a wide range of specific controls required by U.S. government agencies. AWS compliance with these general standards provides customers with in-depth information on the comprehensive nature of the controls and security processes in place in the AWS Cloud.

AWS Global Regions

The AWS Cloud infrastructure is built around regions and *availability zones*. A region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible using a single data center.

As of this writing, the AWS Cloud operates 33 Availability Zones within 12 geographic regions around the world. The 12 regions are US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Frankfurt), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), China (Beijing), and South America (Sao Paulo).

AWS Risk and Compliance Program

AWS Risk and Compliance is designed to build on traditional programs and help customers establish and operate in an AWS security control environment. AWS provides detailed information about its risk and compliance program to enable customers to incorporate AWS controls into their governance frameworks. This information can assist customers in documenting complete control and governance frameworks in which AWS is included as an important part.

The three core areas of the risk and compliance program—risk management, control environment, and information security—are described next.

Risk Management

AWS has developed a strategic business plan that includes risk identification and the implementation of controls to mitigate or manage risks. An AWS management team reevaluates the business risk plan at least twice a year. As a part of this process, management team members are required to identify risks within their specific areas of responsibility and implement controls designed to address and perhaps even eliminate those risks.

The AWS control environment is subject to additional internal and external risk assessments. The 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 they have effectively integrated the *ISO 27001* certifiable framework based on ISO 27002 controls, AICPA Trust Services Principles, PCI DSS v3.1, and the *National Institute of Standards and Technology (NIST)*Publication 800–53, Revision 3, Recommended Security Controls for Federal Information Systems. AWS maintains the security policy and provides security training to its employees. Additionally, AWS performs regular application security reviews to assess the confidentiality, integrity, and availability of data, and conformance to the information security policy.

The AWS security team regularly scans any public-facing endpoint IP addresses for vulnerabilities. It is important to understand that these scans do not include customer instances. AWS security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, independent security firms regularly perform external vulnerability threat assessments. 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 that are required to meet their specific compliance requirements.

As mentioned in Chapter 12, customers can request permission to conduct their own vulnerability scans on their own environments. These vulnerability scans must not violate the AWS acceptable use policy, and they must be requested in advance of the scan.

Control Environment

AWS manages a comprehensive control environment that consists of policies, processes, and control activities. This control environment is in place for the secure delivery of AWS service

offerings. The collective control environment includes 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 environments.

The control environment at AWS 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 for employees commensurate with the employee's position and level of access to AWS facilities. The company follows a structured onboarding process to familiarize new employees with Amazon tools, processes, systems, policies, and procedures.

Information Security

AWS uses a formal information security program that is designed to protect the confidentiality, integrity, and availability of customers' systems and data. AWS publishes several security whitepapers that are available on the main AWS website. These whitepapers are recommended reading prior to taking the AWS Solutions Architect Associate exam.

AWS Reports, 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. A high-level description of the various AWS reports, certifications, and attestations is provided here.

- ***Criminal Justice Information Services (CJIS)***—AWS complies with the Federal Bureau of Investigation's (FBI) CJIS standard. AWS signs CJIS security agreements with AWS customers, which include allowing or performing any required employee background checks according to the CJIS security policy.
- ***Cloud Security Alliance (CSA)***—In 2011, the CSA launched the Security, Trust, & Assurance Registry (STAR), an initiative to encourage transparency of security practices within cloud providers. CSA STAR is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or with whom they are considering contracting. AWS is a CSA STAR registrant and has completed the CSA Consensus Assessments Initiative Questionnaire (CAIQ).
- ***Cyber Essentials Plus***—Cyber Essentials Plus is a UK government-backed, industry-supported certification schema introduced in the UK to help organizations demonstrate operational security against common cyber-attacks. It demonstrates the baseline controls that AWS implements to mitigate the risk from common Internet-based threats within the context of the UK government's "10 Steps to Cyber Security." It is backed by industry, including the Federation of Small Businesses, the Confederation of British Industry, and a number of insurance organizations that offer incentives for businesses holding this certification.
- ***Department of Defense (DoD) Cloud Security Model (SRG)***—The DoD SRG provides a formalized assessment and authorization process for Cloud Service Providers (CSPs) to gain a DoD provisional authorization, which can subsequently be leveraged by DoD customers. A provisional authorization under the SRG provides a reusable certification that attests to AWS compliance with DoD standards, reducing the time necessary for a DoD mission owner to assess and authorize one of their systems for operation on AWS. As of this writing, AWS holds provisional authorizations at Levels 2 (all AWS US-based regions) and 4 (AWS GovCloud [US]) of the SRG.
- ***Federal Risk and Authorization Management Program (FedRAMP)***—AWS is a FedRAMP-compliant CSP. AWS has completed the testing performed by a FedRAMP-accredited third-party assessment organization (3PAO) and has been granted two Agency Authority to Operate (ATOs) by the U.S. Department of Health and Human Services (HHS) after demonstrating compliance with FedRAMP requirements at the moderate impact level.
- ***Family Educational Rights and Privacy Act (FERPA)***—FERPA (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to

their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students." AWS enables covered entities and their business associates subject to FERPA to leverage the secure AWS environment to process, maintain, and store protected education information.

- ***Federal Information Processing Standard (FIPS)*** 140–2—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, Secure Sockets Layer (SSL) terminations 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 when using the AWS GovCloud (US) environment.
- ***FISMA and DoD Information Assurance Certification and Accreditation Process (DIACAP)***—AWS enables U.S. government agencies to achieve and sustain compliance with 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 DoD organizations have successfully achieved security authorizations for systems hosted on AWS in accordance with the Risk Management Framework (RMF) process defined in NIST 800–37 and DIACAP.
- ***Health Insurance Portability and Accountability Act (HIPAA)***—AWS enables covered entities and their business associates subject to HIPAA to leverage the secure AWS environment to process, maintain, and store protected health information. AWS signs business associate agreements with such customers.
- ***Information Security Registered Assessors Program (IRAP)***—IRAP enables Australian government customers to validate that appropriate controls are in place and determine the appropriate responsibility model for addressing the needs of the Australian Signals Directorate (ASD) Information Security Manual (ISM). AWS has completed an independent assessment that has determined that all applicable ISM controls are in place relating to the processing, storage, and transmission of Unclassified Dissemination Limiting Marker (DLM) workloads for the Asia Pacific (Sydney) region.
- ***ISO 9001***—AWS has achieved ISO 9001 certification. AWS ISO 9001 certification directly supports customers who develop, migrate, and operate their quality-controlled IT systems in the AWS Cloud. Customers can leverage AWS compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as Good Laboratory, Clinical, or Manufacturing Practices (GxP) in life sciences, ISO 13485 in medical devices, AS9100 in aerospace, and ISO Technical Specification (ISO/TS) 16949 in the automotive industry. AWS customers who don't have quality system requirements can still benefit from the additional assurance and transparency that an ISO 9001 certification provides.
- ***ISO 27001***—AWS has achieved ISO 27001 certification of the Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services that are detailed in the AWS Risk and Compliance whitepaper, available on the AWS website.
- ***ISO 27017***—ISO 27017 is the newest code of practice released by ISO. It provides implementation guidance on information security controls that specifically relate to

cloud services. AWS has achieved ISO 27017 certification of the ISMS covering AWS infrastructure, data centers, and services that are detailed in the AWS Risk and Compliance whitepaper, available on the AWS website.

- ***ISO 27018***—This is the first international code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002, and it provides implementation guidance on ISO 27002 controls applicable to public cloud-related Personally Identifiable Information (PII). It also provides a set of controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. AWS has achieved ISO 27018 certification of the AWS ISMS covering AWS infrastructure, data centers, and services that are detailed in the AWS Risk and Compliance whitepaper, available on the AWS website.
- ***U.S. International Traffic in Arms Regulations (ITAR)***—The AWS GovCloud (US) region supports 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 U.S. persons and restricting physical location of that data to the U.S. AWS GovCloud (US) provides an environment physically located in the United States where access by AWS personnel is limited to U.S. persons, thereby allowing qualified companies to transmit, process, and store protected articles and data subject to ITAR restrictions. The AWS GovCloud (US) environment has been audited by an independent third party to validate that the proper controls are in place to support customer export compliance programs for this requirement.
- ***Motion Picture Association of America (MPAA)***—MPAA has established a set of best practices for securely storing, processing, and delivering protected media and content. 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 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.
- ***Multi-Tier Cloud Security (MTCS) Tier 3 Certification***—MTCS is an operational Singapore security management standard (SPRING SS 584:2013) based on the ISO 27001/02 ISMS standards.
- ***NIST***—In June 2015, NIST released guideline 800–171, Final Guidelines for Protecting Sensitive Government Information Held by Contractors. This guidance is applicable to the protection of Controlled Unclassified Information (CUI) on non-federal systems. AWS is already compliant with these guidelines, and customers can effectively comply with NIST 800–171 immediately. NIST 800–171 outlines a subset of the NIST 800–53 requirements, a guideline under which AWS has already been audited under the FedRAMP program. The FedRAMP moderate security control baseline is more rigorous than the recommended requirements established in NIST 800–171, and it includes a significant number of security controls above and beyond those required of FISMA moderate systems that protect CUI data.
- ***PCI DSS Level 1***—AWS is Level 1-compliant under PCI DSS. Customers can run

applications on the AWS PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. In February 2013, the PCI Security Standards Council released the PCI DSS cloud computing guidelines. These guidelines provide customers who are managing a cardholder data environment with considerations for maintaining PCI DSS controls in the cloud. AWS has incorporated the PCI DSS cloud computing guidelines into the AWS PCI compliance package for customers.

- ***SOC 1/International Standards for Assurance Engagements No. 3402 (ISAE 3402)***—AWS publishes a SOC 1, Type II report. The audit for this report is conducted in accordance with AICPA: AT 801 (formerly Statement on Standards for Attestation Engagements No. 16 [SSAE 16]) and ISAE 3402). 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 report is the replacement of the SAS 70, Type II audit report.
- ***SOC 2***—In addition to the SOC 1 report, AWS publishes a SOC 2, Type II report. Similar to 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 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 AWS controls that meet the criteria for the security and availability principles set forth in the AICPA trust services principles criteria. The report provides additional transparency into AWS security and availability based on a predefined 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.
- ***SOC 3***—AWS publishes a SOC 3 report. The SOC 3 report is a publicly available summary of the AWS SOC 2 report. The report includes the external auditor's opinion of the operation of controls (based on the AICPA security trust principles included in the SOC 2 report), the assertion from AWS management regarding the effectiveness of controls, and an overview of AWS infrastructure and services. The AWS SOC 3 report includes all AWS data centers worldwide that support in-scope services. This is a great resource for customers to validate that AWS has obtained external auditor assurance without going through the process of requesting a SOC 2 report. The SOC 3 report covers the same services covered in the SOC 1 report.

Summary

AWS communicates with customers regarding its security and control environment through the following mechanisms:

- Obtaining industry certifications and independent third-party attestations
- Publishing information about security and AWS control practices via the website, whitepapers, and blogs
- Directly providing customers with certificates, reports, and other documentation (under NDA in some cases)

The shared responsibility model is not just limited to security considerations; it also extends to IT controls. The management, operation, and verification of IT controls are shared between AWS and the customer. AWS manages these controls where it relates to the physical infrastructure, and the customer manages these controls for the guest operating systems and upward (depending on the service).

It is the customer's responsibility to maintain adequate governance over the entire IT control environment, regardless of how their IT is deployed (on-premises, cloud, or hybrid). By deploying to the AWS Cloud, customers have different options for applying different types of controls and various verification methods that align with their business requirements.

The control environment for AWS contains a large volume of information. This information is provided to customers through whitepapers, reports, certifications, and other third-party attestations. AWS provides IT control information to customers in two ways: specific control definition and general control standard compliance.

AWS provides documentation about its risk and compliance program. This documentation can enable customers to include AWS controls in their governance frameworks. The three core areas of the risk and compliance program are risk management, control environment, and information security.

AWS has achieved a number of internationally recognized certifications and accreditations that demonstrate AWS compliance with third-party assurance frameworks, including:

- FedRAMP
- FIPS 140–2
- FISMA and DIACAP
- HIPAA
- ISO 9001
- ISO 27001
- ITAR
- PCI DSS Level 1
- SOC 1/ISAE 3402
- SOC 2

- SOC 3

AWS is constantly listening to customers and examining other certifications for the future.

Exam Essentials

Understand the shared responsibility model. The shared responsibility model is not just limited to security considerations; it also extends to IT controls. For example, the management, operation, and verification of IT controls are shared between AWS and the customer. AWS manages these controls where it relates to physical infrastructure.

Remember that IT governance is the customer's responsibility. It is the customer's responsibility to maintain adequate governance over the entire IT control environment, regardless of how its IT is deployed (on-premises, cloud, or hybrid).

Understand how AWS provides control information. AWS provides IT control information to customers in two ways: via specific control definition and through a more general control standard compliance.

Remember that AWS is very proactive about risk management. AWS takes risk management very seriously, so it has developed a business plan to identify any risks and to implement controls to mitigate or manage those risks. An AWS management team reevaluates the business risk plan at least twice a year. As a part of this process, management team members are required to identify risks within their specific areas of responsibility and then implement controls designed to address and perhaps even eliminate those risks.

Remember that the control environment is not just about technology. The AWS control environment consists of policies, processes, and control activities. This control environment includes people, processes, and technology.

Remember the key reports, certifications, and third-party attestations. The key reports, certifications, and third-party attestations include, but are not limited to, the following:

- FedRAMP
- FIPS 140–2
- FISMA and DIACAP
- HIPAA
- ISO 9001
- ISO 27001
- ITAR
- PCI DSS Level 1
- SOC 1/ISAE 3402
- SOC 2
- SOC 3

Review Questions

1. AWS communicates with customers regarding its security and control environment through a variety of different mechanisms. Which of the following are valid mechanisms? (Choose 3 answers)
   A. Obtaining industry certifications and independent third-party attestations
   B. Publishing information about security and AWS control practices via the website, whitepapers, and blogs
   C. Directly providing customers with certificates, reports, and other documentation (under NDA in some cases)
   D. Allowing customers' auditors direct access to AWS data centers, infrastructure, and senior staff
2. Which of the following statements is true when it comes to the AWS shared responsibility model?
   A. The shared responsibility model is limited to security considerations only; it does not extend to IT controls.
   B. The shared responsibility model is only applicable for customers who want to be compliant with SOC 1 Type II.
   C. The shared responsibility model is not just limited to security considerations; it also extends to IT controls.
   D. The shared responsibility model is only applicable for customers who want to be compliant with ISO 27001.
3. AWS provides IT control information to customers in which of the following ways?
   A. By using specific control definitions or through general control standard compliance
   B. By using specific control definitions or through SAS 70
   C. By using general control standard compliance and by complying with ISO 27001
   D. By complying with ISO 27001 and SOC 1 Type II
4. Which of the following is a valid report, certification, or third-party attestation for AWS? (Choose 3 answers)
   A. SOC 1
   B. PCI DSS Level 1
   C. SOC 4
   D. ISO 27001
5. Which of the following statements is true?
   A. IT governance is still the customer's responsibility, despite deploying their IT estate onto the AWS platform.

B. The AWS platform is PCI DSS-compliant to Level 1. Customers can deploy their web applications to this platform, and they will be PCI DSS-compliant automatically.

C. The shared responsibility model applies to IT security only; it does not relate to governance.

D. AWS doesn't take risk management very seriously, and it's up to the customer to mitigate risks to the AWS infrastructure.

6. Which of the following statements is true when it comes to the risk and compliance advantages of the AWS environment?

A. Workloads must be moved entirely into the AWS Cloud in order to be compliant with various certifications and third-party attestations.

B. The critical components of a workload must be moved entirely into the AWS Cloud in order to be compliant with various certifications and third-party attestations, but the non-critical components do not.

C. The non-critical components of a workload must be moved entirely into the AWS Cloud in order to be compliant with various certifications and third-party attestations, but the critical components do not.

D. Few, many, or all components of a workload can be moved to the AWS Cloud, but it is the customer's responsibility to ensure that their entire workload remains compliant with various certifications and third-party attestations.

7. Which of the following statements best describes an Availability Zone?

A. Each Availability Zone consists of a single discrete data center with redundant power and networking/connectivity.

B. Each Availability Zone consists of multiple discrete data centers with redundant power and networking/connectivity.

C. Each Availability Zone consists of multiple discrete regions, each with a single data center with redundant power and networking/connectivity.

D. Each Availability Zone consists of multiple discrete data centers with shared power and redundant networking/connectivity.

8. With regard to vulnerability scans and threat assessments of the AWS platform, which of the following statements are true? (Choose 2 answers)

A. AWS regularly performs scans of public-facing endpoint IP addresses for vulnerabilities.

B. Scans performed by AWS include customer instances.

C. AWS security notifies the appropriate parties to remediate any identified vulnerabilities.

D. Customers can perform their own scans at any time without advance notice.

9. Which of the following best describes the risk and compliance communication responsibilities of customers to AWS?

A. AWS and customers both communicate their security and control environment

information to each other at all times.

B. AWS publishes information about the AWS security and control practices online, and directly to customers under NDA. Customers do not need to communicate their use and configurations to AWS.

C. Customers communicate their use and configurations to AWS at all times. AWS does not communicate AWS security and control practices to customers for security reasons.

D. Both customers and AWS keep their security and control practices entirely confidential and do not share them in order to ensure the greatest security for all parties.

10. When it comes to risk management, which of the following is true?

A. AWS does not develop a strategic business plan; risk management and mitigation is entirely the responsibility of the customer.

B. AWS has developed a strategic business plan to identify any risks and implemented controls to mitigate or manage those risks. Customers do not need to develop and maintain their own risk management plans.

C. AWS has developed a strategic business plan to identify any risks and has implemented controls to mitigate or manage those risks. Customers should also develop and maintain their own risk management plans to ensure they are compliant with any relevant controls and certifications.

D. Neither AWS nor the customer needs to worry about risk management, so no plan is needed from either party.

11. The AWS control environment is in place for the secure delivery of AWS Cloud service offerings. Which of the following does the collective control environment NOT explicitly include?

A. People

B. Energy

C. Technology

D. Processes

12. Who is responsible for the configuration of security groups in an AWS environment?

A. The customer and AWS are both jointly responsible for ensuring that security groups are correctly and securely configured.

B. AWS is responsible for ensuring that all security groups are correctly and securely configured. Customers do not need to worry about security group configuration.

C. Neither AWS nor the customer is responsible for the configuration of security groups; security groups are intelligently and automatically configured using traffic heuristics.

D. AWS provides the security group functionality as a service, but the customer is responsible for correctly and securely configuring their own security groups.

13. Which of the following is NOT a recommended approach for customers trying to achieve strong compliance and governance over an entire IT control environment?

    A. Take a holistic approach: review information available from AWS together with all other information, and document all compliance requirements.

    B. Verify that all control objectives are met and all key controls are designed and operating effectively.

    C. Implement generic control objectives that are not specifically designed to meet their organization's compliance requirements.

    D. Identify and document controls owned by all third parties.