Jonathan Anderson

AWS

Certified Solutions Architect

Associate

The ultimate guide for the

SAA-C03

Imagen que contiene lego, juguete

Descripción generada automáticamenteE X A M

**AWS Risk and Compliance Program**

AWS proporciona información sobre su programa de conformidad y administración de riesgos para permitir a los clientes integrar los controles de AWS en su marco de gobierno. Con AWS como parte integral del proceso, este conocimiento ayudará a los clientes a documentar una sólida estructura de gobierno y control.

## Risk Management

La administración de AWS ha establecido una estrategia empresarial proactiva que requiere la detección de amenazas y la implementación de controles de administración o reducción de riesgos. La administración de AWS vuelve a evaluar el plan estratégico de negocios al menos dos veces al año. Este proceso requiere que la gerencia identifique los riesgos en sus áreas de responsabilidad e implemente medidas apropiadas para abordar esos riesgos.

Además, el entorno de monitoreo de AWS está sujeto a diferentes evaluaciones de riesgos internas y externas. Los equipos de administración y conformidad de AWS han desarrollado una política de seguridad de la información y políticas centradas en la política de objetivos de control de la información y la tecnología asociada (COBIT) y han implementado de manera efectiva el marco certificable ISO 27001 basado en ISO 27002 auditorías, Estándares de Servicios Fiduciarios del Instituto Americano de Contadores Públicos Certificados (AICPA), PCI DSS v3.1 y National Institute v3.1 Información del gobierno federal). AWS aplica políticas de seguridad, proporciona al personal capacitación en seguridad y realiza pruebas de seguridad de aplicaciones. Estas evaluaciones analizan la protección, honestidad y disponibilidad de los datos, así como el cumplimiento de las políticas sobre seguridad de la información.

AWS Security analiza periódicamente todas las direcciones IP de los puntos de enlace de servicios de Internet en busca de vulnerabilidades (estos análisis no incluyen instancias de cliente). AWS Security notifica a las partes adecuadas para corregir las vulnerabilidades identificadas. Además, los análisis de amenazas externas son realizados regularmente por compañías de seguridad independientes. Las conclusiones y recomendaciones resultantes de estas evaluaciones se clasifican y se envían a la administración de AWS. Estos análisis se realizan para garantizar la integridad y viabilidad de la infraestructura de AWS subyacente y no están destinados a reemplazar los análisis de vulnerabilidades del cliente necesarios para cumplir con sus requisitos de conformidad específicos.

**Control Management**

AWS mantiene un entorno de control sólido que implica políticas, procedimientos y actividades de control que explotan diferentes facetas del entorno de control general de Amazon. Para la entrega segura de las ofertas de servicios de AWS, se implementa este entorno controlado. El entorno de control colectivo incluye los individuos, los procedimientos y las tecnologías necesarios para crear y mantener un entorno que admita la eficacia operativa del marco de control de AWS. AWS ha incluido controles específicos de la nube aplicables identificados por organizaciones líderes en la industria de la computación en la nube como parte del marco de control de AWS. AWS continúa siguiendo a estos grupos de la industria en busca de ideas relacionadas con prácticas líderes en la industria que se pueden implementar para ayudar a los clientes a administrar mejor su entorno de control.

El entorno de control de Amazon comienza en el nivel superior de la empresa. El liderazgo y la alta dirección juegan un papel importante en el establecimiento del tono y los valores fundamentales de la empresa. Cada empleado recibe el código de conducta y ética de la empresa y toma cursos de capacitación periódicos. Las auditorías de cumplimiento se llevan a cabo para que los empleados entiendan y sigan las políticas establecidas.

La estructura organizativa de AWS proporciona un sistema para organizar, dirigir y administrar las actividades empresariales. Para garantizar una dotación de personal adecuada, operaciones eficaces y la separación de funciones, la estructura organizativa asigna funciones y responsabilidades. La administración también ha establecido la autoridad y las líneas jerárquicas apropiadas para el personal clave. Los procesos de verificación de contratación de la compañía incluyen capacitación, empleo previo y, en algunos casos, verificación de antecedentes, según lo permitido por la ley y la regulación, para los empleados y esto se basa en sobre la posición de la empresa, el nivel de los empleados y el nivel de acceso a las instalaciones de AWS.

## Information Security

Para proteger la integridad, confidencialidad y disponibilidad de los sistemas y datos de los clientes, AWS ha introducido una política estructurada de seguridad de la información. AWS publica un documento técnico de seguridad en su sitio web público que explica cómo AWS puede ayudar a los clientes a mantener sus datos seguros.

## AWS Contact

Los clientes pueden enviar informes y certificaciones preparados por nuestros auditores externos o poniéndose en contacto con AWS Sales and Business Development para enviar más información sobre la conformidad con AWS. El representante remitirá a los clientes al equipo apropiado en función de la naturaleza de la investigación. Para obtener más información sobre la conformidad con AWS, visite el sitio de conformidad de AWS o envíe sus preguntas directamente a mailto: [awscompliance@amazon.com.](mailto:awscompliance@amazon.com)

## Essential Exam

* 1. Comprender el modelo de responsabilidad compartida. El modelo de responsabilidad compartida no se limita a consideraciones de seguridad; también se extiende a las auditorías de TI. Por ejemplo, la administración, el funcionamiento y la verificación de los controles de TI se comparten entre AWS y el cliente. AWS aplica estos controles con respecto a la infraestructura física.
  2. Recuerde que el gobierno de TI es responsabilidad del cliente. El cliente es responsable de garantizar una gestión adecuada de toda la configuración de control de TI, independientemente de cómo se implemente la TI (en las instalaciones, en la nube o híbrida).
  3. Comprenda cómo AWS proporciona información de monitoreo. AWS entrega información de control de TI a los clientes de dos maneras: a través de una definición de control específica y mediante el cumplimiento de estándares de control más generales.
  4. Recuerde, AWS es muy proactivo cuando se trata de la administración de riesgos. AWS se toma muy en serio la administración de riesgos y, por lo tanto, ha desarrollado un plan de negocios para identificar riesgos e implementar controles para mitigar o administrar esos riesgos. Un equipo de liderazgo de AWS vuelve a evaluar el plan de administración de riesgos corporativo al menos dos veces al año.
  5. Se espera que los miembros del equipo de gestión reconozcan los riesgos en sus respectivas áreas de responsabilidad como parte de este proceso y luego hagan cumplir los controles diseñados para resolver y tal vez incluso descartar esos riesgos.
  6. Recuerde que el entorno de control no se basa únicamente en la tecnología. La regulación, los procedimientos y las operaciones de monitoreo se incluyen en el sistema de control de AWS. Las personas, los procedimientos y las tecnologías se incluyen en esta configuración de control.
  + No olvide informes importantes, certificaciones y atestaciones de terceros. Los informes, certificaciones y atestaciones importantes de terceros incluyen, entre otros, los siguientes:

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 about its security and control environment through various mechanisms. Which of the following are valid mechanisms? (Choose 3 answers)
2. Obtain industrial certifications and independent third-party representations
3. Post information about AWS security and auditing practices through the website, white papers and blogs
4. Provide certificates, reports and other documents directly to customers (in some cases under NDA)
5. Provide customer auditors direct access to AWS data centers, infrastructure and senior management
6. Which of the following statements about the AWS Model of Shared Responsibility is true?
   1. The paradigm of shared accountability is restricted to safety considerations; it does not extend to computer controllers.
   2. The shared responsibility model only applies to customers that are willing to comply with the SOC 1 Type II.
   3. The model of shared responsibility is not limited to security considerations; it also extends to IT audits.
   4. The shared responsibility model only applies to customers who wish to comply with ISO 27001.
7. AWS delivers IT control information to customers in any of the following ways?
   1. Using specific audit definitions or following common auditing standards
   2. Use of specific audit definitions or through SAS 70
   3. Compliance with general principles of auditing and in accordance with ISO 27001
   4. By meeting the requirements of ISO 27001 and SOC 1 Type II
8. What is a valid third party report, certification or attestation for AWS? (Choose 3 answers)
   1. SOC 1
   2. PCI DSS level 1
   3. SOC 4
   4. ISO 27001
9. Which of the following statements is true?
10. IT governance is still the responsibility of the customer, despite the implementation of their IT infrastructure on the AWS platform.
11. The AWS platform is PCI DSS Level 1 compliant. Customers can deploy their web applications on this platform and will automatically be PCI DSS compliant.
12. The shared responsibility model applies only to IT security; it's not about governance.
13. AWS does not take risk management very seriously, and it is the customer's responsibility to mitigate risk to the AWS infrastructure.
14. Which of the following statements is true about the risks and compliance benefits of the AWS environment?
    1. Workloads must be fully moved to the AWS Cloud to comply with various third-party certifications and attestations.
    2. Critical components of a workload must be fully moved to the AWS Cloud to comply with various third-party certifications and attestations, but not non- critical components.
    3. Non-critical components of a workload must be completely moved to the AWS Cloud to meet various third-party certifications and attestations, but critical components must not be moved.
    4. Few, several, or all components of a workload may be transferred to the AWS Cloud, but the customer must ensure that their whole workload continues to comply with various certifications and certificates from third parties.
15. Which of the definitions better describes a zone of availability?
16. A single, distinct data center with redundant power and network/connectivity consists of each availability zone.
17. Two discrete data centers with redundant power and network/connectivity consist of each availability region.
18. Each zone of availability consists of many distinct zones, each with redundant power and network/communication data center.
19. Multiple distinct data centers with shared power and redundant network/connectivity consist of each availability region.
20. As for the AWS platform's vulnerability scanning and threat analysis, which of the following statements is true? (Choose 2 answers)
21. AWS regularly scans the IP addresses of publicly available endpoints for vulnerabilities.
22. Scans performed by AWS include customer instances.
23. AWS Security notifies the appropriate parties to fix identified vulnerabilities.
24. Customers may perform their own analysis at any time without notice.
25. Which of the following best describes customer risk communications and compliance responsibilities for AWS?
26. AWS and customers share information about their security and control environment at all times.
27. AWS publishes information about AWS security and auditing practices online and directly to customers under NDA. Customers do not need to report their usage and configurations to AWS.
28. Customers communicate their usage and configurations to AWS at all times. AWS does not communicate AWS security and auditing practices to customers for security reasons.
29. Customers and AWS retain their entirely proprietary protection and control procedures and do not disclose them to ensure the highest form of protection for both parties.
30. In respect to risk management, which of the below statements is true?
    1. AWS does not formulate a strategic business plan; the client is solely responsible for risk control and risk management.
    2. In order to define threats and enforce controls to reduce or handle those threats, AWS has established a strategic business plan. Customers do not have to create and manage their own risk management programs.
    3. In order to define threats, AWS has built a strategic business plan and has developed controls to reduce or handle those threats. Customers must also develop and maintain their own risk management plans to ensure that they comply with all relevant controls and certifications.
    4. Neither AWS nor the customer need to worry about managing risk, so no plan is needed to be developed on both sides.
31. For the safe distribution of AWS Cloud services, the AWS control environment should be in place. In the collective control setting, which of the following is NOT expressly included?

A people

1. Energy
2. Technology
3. Process
4. In an AWS environment, who is responsible for setting up security groups?
   1. The customer and AWS are collectively responsible for ensuring the correct and stable configuration of security classes.
   2. AWS is responsible for ensuring the correct and stable configuration of all security classes. There's no need for clients to think about setting up a protection squad.
   3. Neither AWS nor Customer is responsible for configuring security groups; security groups are intelligently and automatically configured using traffic heuristics.
   4. AWS provides Security Group as a Service functionality, but the Customer is responsible for the correct and secure configuration of its security groups.
5. Which of the option is NOT a recommended approach for customers seeking strong compliance and governance for a full IT control environment?
   1. Take a holistic approach: Review the information available on AWS along with all other information and document all compliance requirements.
   2. Verify that all control objectives have been met and that all significant controls have been designed and are operating effectively.
   3. Implement generic audit objectives that are not specifically designed to meet their organization's compliance requirements.
   4. Identify and document controls from all third parties.

## Answers to Review Questions

* + 1. A, B, C. Answers A through C define legitimate methods used by AWS to communicate with customers about its protection and control environment. AWS does not provide direct access to AWS data centers, facilities, or personnel for customer auditors.
    2. C. The shared responsibility model can include IT controls, and it is not limited to security considerations. Therefore, answer C is correct.
    3. A. AWS provides IT control information to customers through either specific control definitions or general control standard compliance.
    4. A, B, D. There is no such thing as a SOC 4 report, therefore, answer C is incorrect.
    5. A. IT governance still remains the customer's responsibility.
    6. D. Any number of workload components can be migrated to AWS, but it is the duty of the client to ensure that the whole workload remains consistent with different certifications and certifications from third parties.
    7. B. There are several discrete data centers in an Availability Region, each with its own redundant power and network / connectivity, therefore, B is the right answer.
    8. A, C. AWS periodically scans and notifies relevant parties of public-facing, non-customer endpoint IP addresses. AWS does not scan client instances, and clients need to ask for the right to conduct their own scans in advance, so responses A and C are accurate.
    9. B. AWS publishes information publicly online and directly to NDA customers, but customers are not expected to share information about their usage and configuration with AWS, therefore, B is right answer.
    10. C. AWS has developed a strategic business plan, and clients can also build and sustain their own risk management plans, so C is the correct answer.
    11. B. The collective control environment involves the individuals, processes and technologies required to build and sustain an environment that supports the AWS control framework's operating performance. Energy is not a part of the control environment that is discretely defined, so B is the correct response.
    12. D. Customers should ensure that all the configurations of their security group are suitable for their own applications; response D is therefore correct.
    13. C. Customers should ensure that they enforce control targets that are tailored to fulfilling the specific compliance criteria of their company, so C is right.