



Isaca CCAK Practice Questions

Shared by Howe on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

An auditor wants to get information about the operating effectiveness of controls addressing privacy, availability, and confidentiality of a service organization. Which of the following can BEST help to gain the required information?

Options:

- A- ISAE 3402 report
- B- ISO/IEC 27001 certification
- C- SOC1 Type 1 report
- D- SOC2 Type 2 report

Answer:

D

Explanation:

A SOC2 Type 2 report can best help an auditor to get information about the operating effectiveness of controls addressing privacy, availability, and confidentiality of a service organization. A SOC2 Type 2 report is an internal control report that examines the security, availability, processing integrity, confidentiality, and privacy of a service organization's system and data over a specified period of time, typically 3-12 months. A SOC2 Type 2 report is based on the AICPA Trust Services Criteria and provides an independent auditor's opinion on the design and operating effectiveness of the service organization's controls. A SOC2 Type 2 report can help an auditor to assess the risks and challenges associated with outsourcing services to a cloud provider and to verify that the provider meets the relevant compliance requirements and industry standards.¹²Reference: = CCAK Study Guide, Chapter 5: Cloud Auditing, page 971; SOC 2 Type II Compliance: Definition, Requirements, and Why You Need It²

Question 2

Question Type: MultipleChoice

The MOST important factor to consider when implementing cloud-related controls is the:

Options:

- A- shared responsibility model.
- B- effectiveness of the controls.
- C- risk reporting.
- D- risk ownership

Answer:

A

Explanation:

[The most important factor to consider when implementing cloud-related controls is the shared responsibility model. The shared responsibility model is a framework that defines the roles and responsibilities of cloud service providers \(CSPs\) and cloud customers \(CCs\) in ensuring the security and compliance of cloud computing environments. The shared responsibility model helps to clarify which security tasks are handled by the CSP and which tasks are handled by the CC, depending on the type of cloud service model \(IaaS, PaaS, SaaS\) and the specific contractual agreements. The shared responsibility model also helps to avoid gaps or overlaps in security controls, and to allocate resources and accountability accordingly12.](#)

[Shared responsibility in the cloud - Microsoft Azure](#)

[Understanding the Shared Responsibilities Model in Cloud Services - ISACA](#)

Question 3

Question Type: MultipleChoice

Which of the following MOST enhances the internal stakeholder decision-making process for the remediation of risks identified from an organization's cloud compliance program?

Options:

- A- Establishing ownership and accountability
- B- Reporting emerging threats to senior stakeholders
- C- Monitoring key risk indicators (KRIs) for multi-cloud environments
- D- Automating risk monitoring and reporting processes

Answer:

A

Explanation:

The most effective way to enhance the internal stakeholder decision-making process for the remediation of risks identified from an organization's cloud compliance program is to establish ownership and accountability for each risk and its corresponding control. Ownership and accountability mean that the stakeholders who are responsible for managing, implementing, monitoring, and reporting on the cloud compliance program have clearly defined roles, responsibilities, expectations, and authorities. Ownership and accountability also mean that the stakeholders who are affected by or involved in the cloud compliance program have sufficient awareness, communication, collaboration, and feedback mechanisms. Establishing ownership and accountability helps to ensure that the risks and controls are properly identified, assessed, prioritized, treated, and reviewed in a timely and consistent manner. It also helps to foster a culture of trust, transparency, and accountability among the internal stakeholders and to align their goals and interests with the organization's cloud compliance objectives.^{1[2][2]}

Question 4

Question Type: MultipleChoice

Which of the following is a KEY benefit of using the Cloud Controls Matrix (CCM)?

Options:

- A- CCM utilizes an ITIL framework to define the capabilities needed to manage the IT services and security services.
- B- CCM maps to existing security standards, best practices, and regulations.
- C- CCM uses a specific control for Infrastructure as a Service (IaaS).
- D- CCM V4 is an improved version from CCM V3.0.1.

Answer:

B

Explanation:

The Cloud Controls Matrix (CCM) is a cybersecurity control framework specifically designed for cloud computing environments. A key benefit of using the CCM is that it maps to existing security standards, best practices, and regulations. This mapping allows organizations to ensure that their cloud security posture aligns with industry-recognized frameworks, thereby

facilitating compliance and security assurance efforts. The CCM's comprehensive set of control objectives covers all key aspects of cloud technology and provides guidance on which security controls should be implemented by various actors within the cloud supply chain.

Reference= This answer is supported by the information provided in the Cloud Controls Matrix documentation and related resources, which highlight the CCM's alignment with other security standards and its role in helping organizations navigate the complex landscape of cloud security and compliance¹².

Question 5

Question Type: MultipleChoice

Which of the following types of SOC reports BEST helps to ensure operating effectiveness of controls in a cloud service provider offering?

Options:

- A- SOC 3 Type 2
- B- SOC 2 Type 2
- C- SOC 1 Type 1
- D- SOC 2 Type 1

Answer:

B

Explanation:

A SOC 2 Type 2 report is the most comprehensive type of report for cloud service providers, as it evaluates the design and operating effectiveness of a service organization's controls over a period of time. This type of report is specifically intended to meet the needs of customers who need assurance about the security, availability, processing integrity, confidentiality, or privacy of the data processed by the service provider¹²³⁴.

Reference= The importance of SOC 2 Type 2 reports for cloud service providers is discussed in various resources, including those provided by ISACA and the Cloud Security Alliance, which highlight the need for such reports to ensure the operating effectiveness of controls⁵⁶⁷⁸.

Question 6

Question Type: MultipleChoice

Which of the following is a cloud-native solution designed to counter threats that do not exist within the enterprise?

Options:

- A- Rule-based access control
- B- Attribute-based access control
- C- Policy-based access control
- D- Role-based access control

Answer:

C

Explanation:

Attribute-based access control (ABAC) is a cloud-native solution that uses attributes (such as user role, location, or device) to dynamically control access. This method is highly flexible for the cloud, where user attributes and environmental factors vary, unlike traditional enterprise security models. ISACA's CCAK emphasizes ABAC in cloud environments for its adaptability to multi-tenant architectures and complex access control requirements, aligning with CCM controls in Domain IAM-12 (Identity and Access Management) for flexible, secure access mechanisms.

Question 7

Question Type: MultipleChoice

Which of the following activities are part of the implementation phase of a cloud assurance program during a cloud migration?

Options:

- A- Development of the monitoring goals and requirements
- B- Identification of processes, functions, and systems
- C- Identification of roles and responsibilities

D- Identification of the relevant laws, regulations, and standards

Answer:

A

Explanation:

During the implementation phase of a cloud assurance program, the focus is on establishing the operational aspects that will ensure the ongoing security and compliance of the cloud environment. This includes developing the monitoring goals and requirements which are essential for setting up the assurance framework. It involves determining what needs to be monitored, how it should be monitored, and the metrics that will be used to measure compliance and performance.

Reference= The information aligns with best practices for cloud migration and assurance programs as outlined in various resources, including the Cloud Assurance Program Guide by Microsoft Cybersecurity¹, which discusses the importance of developing and implementing policies for cloud data and system migration, and the Enterprise Guide to Successful Cloud Adoption by New Relic², which emphasizes the role of observability in cloud migration, including the establishment of monitoring goals.

Question 8

Question Type: MultipleChoice

The FINAL decision to include a material finding in a cloud audit report should be made by the:

Options:

A- auditee's senior management.

B- organization's chief executive officer (CEO).

C- cloud auditor.

: D. organization's chief information security officer (CISO)

Answer:

C

Explanation:

According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, the final decision to include a material finding in a cloud audit report should be made by the cloud auditor1. A material finding is a significant error or risk in the cloud service that could affect the achievement of the audit objectives or the cloud customer's business outcomes. The cloud auditor is responsible for identifying, evaluating, and reporting the material findings based on the audit criteria, methodology, and evidence. The cloud auditor should also communicate the material findings to the auditee and other relevant stakeholders, and obtain their feedback and responses.

The other options are not correct. Option A is incorrect, as the auditee's senior management is not in charge of the audit report, but rather the subject of the audit. The auditee's senior management should provide their perspective and action plans for the material findings, but they cannot decide whether to include or exclude them from the report. Option B is incorrect, as the organization's CEO is not involved in the audit process, but rather the ultimate recipient of the audit report. The organization's CEO should review and act upon the audit report, but they cannot influence the content of the report. Option D is incorrect, as the organization's CISO is not an independent party, but rather a stakeholder of the audit. The organization's CISO should support and collaborate with the cloud auditor, but they cannot make the final decision on the material findings. Reference:

[ISACA Cloud Auditing Knowledge Certificate Study Guide, page 19-20.](#)



To Get Premium Files for CCAK Visit

<https://www.p2pexams.com/products/ccak>

For More Free Questions Visit

<https://www.p2pexams.com/isaca/pdf/ccak>

20%
DISCOUNT

P2P
exams