

DUMPSQUEEN

Certificate of Cloud Auditing Knowledge

Isaca CCAK

Version Demo

Total Demo Questions: 10

Total Premium Questions: 126

Buy Premium PDF

<https://dumpsqueen.com>

support@dumpsqueen.com

dumpsqueen.com

QUESTION NO: 1

In which control should a cloud service provider, upon request, inform customers of compliance impact and risk, especially if customer data is used as part of the services?

- A. Service Provider control
- B. Impact and Risk control
- C. Data Inventory control
- D. Compliance control

ANSWER: A

Explanation:

Reference: <https://rmas.fad.harvard.edu/cloud-service-providers>

QUESTION NO: 2

In the context of Infrastructure as a Service (IaaS), a vulnerability assessment will scan virtual machines to identify vulnerabilities in:

- A. both operating system and application infrastructure contained within the CSP's instances.
- B. both operating system and application infrastructure contained within the customer's instances
- C. only application infrastructure contained within the CSP's instances.
- D. only application infrastructure contained within the customer's instances.

ANSWER: C

QUESTION NO: 3

The BEST way to deliver continuous compliance in a cloud environment is to:

- A. decrease the interval between attestations of compliance.
- B. combine point-in-time assurance approaches with continuous monitoring.
- C. increase the frequency of external audits from annual to quarterly.
- D. combine point-in-time assurance approaches with continuous auditing.

ANSWER: B

QUESTION NO: 4

Your company is purchasing an application from a vendor. They do not allow you to perform an on-site audit on their information system. However, they say, they will provide the third-party audit attestation on the adequate control design within their environment. Which report is the vendor providing you?

- A. SOC 3
- B. SOC 2, TYPE 2
- C. SOC 1
- D. SOC 2, TYPE 1

ANSWER: B

Explanation:

Reference: <https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/soc-reports-for-cloud-security-and-privacy>

Figure 3—Comparison of ISO 27001 and SOC 2 Type II Report

Area	ISO 27001/27017	SOC 2 Type II
Standard	International Standard ISO/IEC 27001, Second Edition 2013-10-01, ISMS— <i>Information security management systems</i>	Trust Services Principles and Criteria for Security, Availability, Process Integrity, Confidentiality and/or Privacy
Governing body	American National Standards Institute (ANSI) ANSI-ASQ National Accreditation Board (ANAB)	AICPA
Purpose	Assist organization's management in establishment and certification of ISMS that meets specified requirements and is able to be certified as best practice	Assist service organization's management in reporting to customers that it has met established security criteria that ensure that the system is protected against unauthorized access
Applicability	Statement of Applicability (SOA) of controls	System description by management
Certificate/reporting statement for controls	A point in time, i.e., as on a date	Period of time, i.e., for the period ended XXXX (date)
Objective	Establish, implement, maintain and improve the information security management system (ISMS)	Measure a service organization against specific security principles and criteria
Reporting cycle	Recertified every three years	Attestation provided every year (or six months)
Audit frequency	Surveillance audit conducted annually	Continuous monitoring during the period
Certified/attested by	ISO Accredited Registrar Certification	Attestation by a licensed CPA
Nature of testing	Design effectiveness	Design effectiveness and operating effectiveness
Controls in report	Details of controls not provided	Details of controls provided
Focus	Organization's ability to maintain an ISMS	Technology and the processes behind the applicable trust services criteria of the specific service
Report	Single-page certification	A report containing the auditor's opinion, management's assertion, description of controls, user control considerations, tests of controls and results
Difficulty to achieve	Moderate	Higher
Structure	Information security framework	Principles and criteria

QUESTION NO: 5

The Cloud Computing Compliance Controls Catalogue (C5) framework is maintained by which of the following agencies?

- A. Agence nationale de la sécurité des systèmes d'information (ANSSI)
- B. National Institute of Standards and Technology (NIST)
- C. National Security Agency (NSA)

D. Bundesamt für Sicherheit in der Informationstechnik (BSI)

ANSWER: D

Explanation:

Reference: <https://docs.microsoft.com/en-us/compliance/regulatory/offering-c5-germany>

QUESTION NO: 6

A cloud customer configured and developed a solution on top of the certified cloud services. Building on top of a compliant CSP:

- A. means that the cloud customer is also compliant.
- B. means that the cloud customer and client are both compliant.
- C. means that the cloud customer is compliant but their client is not compliant.
- D. does not necessarily mean that the cloud customer is also compliant.

ANSWER: D

QUESTION NO: 7

Which of the following quantitative measures is KEY for an auditor to review when assessing the implementation of continuous auditing of performance on a cloud system?

- A. Service Level Objective (SLO)
- B. Recovery Point Objectives (RPO)
- C. Service Level Agreement (SLA)
- D. Recovery Time Objectives (RTO)

ANSWER: C

QUESTION NO: 8

Which of the following is the BEST recommendation to offer an organization's HR department planning to adopt a new public SaaS application to ease the recruiting process?

- A. Ensure HIPAA compliance
- B. Implement a cloud access security broker

- C. Consult the legal department
- D. Do not allow data to be in cleartext

ANSWER: B

Explanation:

Reference: <https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-a-casb.html>

A Cloud access security broker, or CASB, is cloud-hosted software or on-premises software or hardware that act as an intermediary between users and cloud service providers. The ability of a CASB to address gaps in security extends across software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) environments. In addition to providing visibility, a CASB also allows organizations to extend the reach of their security policies from their existing on-premises infrastructure to the cloud and create new policies for cloud-specific context.

CASBs have become a vital part of enterprise security, allowing businesses to safely use the cloud while protecting sensitive corporate data.

The CASB serves as a policy enforcement center, consolidating multiple types of security policy enforcement and applying them to everything your business utilizes in the cloud—regardless of what sort of device is attempting to access it, including unmanaged smartphones, IoT devices, or personal laptops.

QUESTION NO: 9

An organization is in the initial phases of cloud adoption. It is not very knowledgeable about cloud security and cloud shared responsibility models. Which of the following approaches is BEST suited for such an organization to evaluate its cloud security?

- A. Use of an established standard/regulation to map controls and use as the audit criteria
- B. For efficiency reasons, use of its on-premises systems' audit criteria to audit the cloud environment
- C. As this is the initial stage, the ISO/IEC 27001 certificate shared by the cloud service provider is sufficient for audit and compliance purposes.
- D. Development of the cloud security audit criteria based on its own internal audit test plans to ensure appropriate coverage

ANSWER: A

QUESTION NO: 10

Which of the following metrics are frequently immature?

- A. Metrics around Infrastructure as a Service (IaaS) storage and network environments
- B. Metrics around Platform as a Service (PaaS) development environments
- C. Metrics around Infrastructure as a Service (IaaS) computing environments

D. Metrics around specific Software as a Service (SaaS) application services

ANSWER: A