

ISACA.CCAK.v2022-02-11.q57

Exam Code:	CCAK
Exam Name:	Certificate of Cloud Auditing Knowledge
Certification Provider:	ISACA
Free Question Number:	57
Version:	v2022-02-11
# of views:	1728
# of Questions views:	570
https://www.exam-tests.com/CCAK-exam/ISACA.CCAK.v2022-02-11.q57.html	

NEW QUESTION: 1

The PRIMARY objective of an audit initiation meeting with a cloud audit client is to:

- A. select the methodology of an audit.
- B. discuss the scope of the cloud audit.
- C. review requested evidence provided by the audit client.
- D. identify resource requirements of the cloud audit.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 2

Segregation of duties would be compromised if:

- A. operations staff modified batch schedules.
- B. application programmers moved programs into production.
- C. database administrators (DBAs) modified the structure of user tables.
- D. application programmers accessed test data.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 3

Which of the following approaches encompasses social engineering of staff, bypassing of physical access controls and penetration testing?

- A. Red team
- B. White box
- C. Gray box
- D. Blue team

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 4

While performing the audit, the auditor found that an object storage bucket containing PII could be accessed by anyone on the Internet. Given this discovery, what should be the most appropriate action for the auditor to perform?

- A.** Documenting the finding in the audit report and sharing the gap with the relevant stakeholders
- B.** Asking the organization's cloud administrator to immediately close the gap by updating the configuration settings and making the object storage bucket private and hence inaccessible from the Internet
- C.** Highlighting the gap to the audit sponsor at the sponsor's earliest possible availability
- D.** Informing the organization's internal audit manager immediately about the gap

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 5

What is true of searching data across cloud environments?

- A.** All cloud-hosted email accounts are easily searchable.
- B.** You might not have the ability or administrative rights to search or access all hosted data.
- C.** Search and discovery time is always factored into a contract between the consumer and provider.
- D.** The cloud provider must conduct the search with the full administrative controls.
- E.** You can easily search across your environment using any E-Discovery tool.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 6

An auditor identifies that a CSP received multiple customer inquiries and RFPs during the last month. Which of the following should be the BEST recommendation to reduce the CSP burden?

- A.** CSP can schedule a call with each customer.
- B.** CSP can answer each customer individually.
- C.** CSP can share all security reports with customers to streamline the process.
- D.** CSP can direct all customers' inquiries to the information in the CSA STAR registry.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

Use elastic servers when possible and move workloads to new instances.

- A.** False
- B.** True

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 8

Which of the following should be the PRIMARY concern of an IS auditor during a review of an external IT service level agreement (SLA) for computer operations?

- A. Lack of software escrow provisions
- B. No employee succession plan
- C. Changes in services are not tracked
- D. Vendor has exclusive control of IT resources

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 9

Which of the following is MOST important to consider when an organization is building a compliance program for the cloud?

- A. The fairly static nature of the service portfolio and architecture of the cloud.
- B. The rapidly changing service portfolio and architecture of the cloud.
- C. Cloud providers should not be part of the compliance program.
- D. The cloud is similar to the on-premise environment in terms of compliance.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 10

Organizations maintain mappings between the different control frameworks they adopt to:

- A. help identify controls with different assessment status.
- B. help identify controls with common assessment status.
- C. avoid duplication of work when assessing compliance.
- D. start a compliance assessment using latest assessment.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 11

How does running applications on distinct virtual networks and only connecting networks as needed help?

- A. It locks down access and provides stronger data security
- B. It reduces the blast radius of a compromised system
- C. It enables you to configure applications around business groups
- D. It provides dynamic and granular policies with less management overhead
- E. It reduces hardware costs

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 12

Which of the following should be the FIRST step to establish a cloud assurance program during a cloud migration?

- A. Development
- B. Stakeholder identification
- C. Risk assessment

D. Design

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 13

Within an organization, which of the following functions should be responsible for defining the cloud adoption approach?

A. Compliance manager

B. IT manager

C. Audit committee

D. Senior management

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 14

An organization recently implemented a cloud document storage solution and removed the ability for end users to save data to their local workstation hard drives Which of the following findings should be the IS auditor's GREATEST concern?

A. The business continuity plan (BCP) was not updated.

B. Users are not required to sign updated acceptable

C. Users have not been trained on the new system.

D. Mobile devices are not encrypted.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 15

In all three cloud deployment models, (IaaS, PaaS, and SaaS), who is responsible for the patching of the hypervisor layer?

A. Cloud service provider

B. Shared responsibility

C. Cloud service customer

D. Patching on hypervisor layer is not required

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 16

Sending data to a provider's storage over an API is likely as much morereliable and secure than setting up your own SFTP server on a VM in the same provider

A. False

B. True

Answer: ([SHOW ANSWER](#))

Valid CCAK Dumps shared by BraindumpsPass.com for Helping Passing CCAK Exam! BraindumpsPass.com now offer the **newest CCAK exam dumps**, the BraindumpsPass.com CCAK exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CCAK dumps with Test Engine here: <https://www.braindumpsPASS.com/ISACA/CCAK-practice-exam-dumps.html> (207 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 17

Which cloud storage technology is basically a virtual hard drive for instanced or VMs?

- A. Application
- B. Platform
- C. Database
- D. Volume storage
- E. Object storage

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 18

Which of the following BEST ensures adequate restriction on the number of people who can access the pipeline production environment?

- A. Ensuring segregation of duties in the production and development pipelines.
- B. Role-based access controls in the production and development pipelines.
- C. Separation of production and development pipelines.
- D. Periodic review of the CI/CD pipeline audit logs to identify any access violations.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 19

Which of the following is NOT a cloud computing characteristic that impacts incidence response?

- A. Privacy concerns for co-tenants regarding the collection and analysis of telemetry and artifacts associated with an incident.
- B. The resource pooling practiced by cloud services, in addition to the rapid elasticity offered by cloud infrastructures.
- C. The on demand self-service nature of cloud computing environments.
- D. Object-based storage in a private cloud.
- E. The possibility of data crossing geographic or jurisdictional boundaries.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 20

Which concept is a mapping of an identity, including roles, personas, and attributes, to an authorization?

- A. Federated Identity Management
- B. Authentication
- C. Access control
- D. Entitlement
- E. Authoritative source

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 21

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 22

A CSP contracts for a penetration test to be conducted on its infrastructures. The auditor engages the target with no prior knowledge of its defenses, assets, or channels. The CSP's security operation center is not notified in advance of the scope of the audit and the test vectors. Which mode is selected by the CSP?

- A. Double blind
- B. Double gray box
- C. Reversal
- D. Tandem

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 23

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. Data Inventory control
- C. Compliance control
- D. Impact and Risk control

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 24

From the perspective of a senior cloud security audit practitioner in an organization of a mature security program with cloud adoption, which of the following statements BEST describes the DevSecOps concept?

- A. Operational framework that promotes software consistency through automation

- B. Development standards for addressing integration, testing, and deployment issues
- C. Making software development simpler, faster, and easier using automation
- D. Process of security integration using automation in software development

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 25

The Cloud Octagon Model was developed to support organizations:

- A. risk assessment methodology.
- B. risk treatment methodology.
- C. incident response methodology.
- D. incident detection methodology.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 26

Which attack surfaces, if any, does virtualization technology introduce?

- A. The hypervisor
- B. All of the above
- C. Virtualization management components apart from the hypervisor
- D. Configuration and VM sprawl issues

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 27

Which of the following should be of GREATEST concern to an IS auditor reviewing actions taken during a forensic investigation?

- A. The investigation report does not indicate a conclusion.
- B. An image copy of the attacked system was not taken.
- C. The handling procedures of the attacked system are not documented.
- D. The proper authorities were not notified.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 28

Which statement best describes the impact of Cloud Computing on business continuity management?

- A. Customers of SaaS providers in particular need to mitigate the risks of application lock-in.
- B. Clients need to do business continuity planning due diligence in case they suddenly need to switch providers.
- C. The size of data sets hosted at a Cloud provider can present challenges if migration to another provider becomes necessary.
- D. A general lack of interoperability standards means that extra focus must be placed on the security aspects of migration between Cloud providers.

E. Geographic redundancy ensures that Cloud Providers provide highly available services.

Answer: E (LEAVE A REPLY)

NEW QUESTION: 29

Which of the following would be the MOST critical finding of an application security and DevOps audit?

- A. Application architecture and configurations did not consider security measures.
- B. The organization is not using a unified framework to integrate cloud compliance with regulatory requirements.
- C. Certifications with global security standards specific to cloud are not reviewed and the impact of noted findings are not assessed.
- D. Outsourced cloud service interruption, breach or loss of data stored at the cloud service provider.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 30

CCM: A hypothetical company called: "Health4Sure" is located in the United States and provides cloud based services for tracking patient health. The company is compliant with HIPAA/HITECH Act among other industry standards. Health4Sure decides to assess the overall security of their cloud service against the CCM toolkit so that they will be able to present this document to potential clients.

Which of the following approach would be most suitable to assess the overall security posture of Health4Sure's cloud service?

- A. The CCM columns are mapped to HIPAA/HITECH Act and therefore Health4Sure could verify the CCM controls already covered as a result of their compliance with HIPAA/HITECH Act. They could then assess the remaining controls. This approach will save time.
- B. The CCM domains are not mapped to HIPAA/HITECH Act. Therefore Health4Sure should assess the security posture of their cloud service against each and every control in the CCM. This approach will allow a thorough assessment of the security posture.
- C. The CCM domain controls are mapped to HIPAA/HITECH Act and therefore Health4Sure could verify the CCM controls already covered as a result of their compliance with HIPAA/HITECH Act. They could then assess the remaining controls thoroughly. This approach saves time while being able to assess the company's overall security posture in an efficient manner.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 31

How is encryption managed on multi-tenant storage?

- A. Multiple keys per data owner
- B. C for data subject to the EU Data Protection Directive; B for all others

- C. Single key for all data owners
- D. The answer could be A, B, or C depending on the provider
- E. One key per data owner

Answer: E ([LEAVE A REPLY](#))

Valid CCAK Dumps shared by BraindumpsPass.com for Helping Passing CCAK Exam! BraindumpsPass.com now offer the **newest CCAK exam dumps**, the BraindumpsPass.com CCAK exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CCAK dumps with Test Engine here: <https://www.braindumpsPASS.com/ISACA/CCAK-practice-exam-dumps.html> (207 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 32

Which of the following is an example of integrity technical impact?

- A. The cloud provider reports a breach of customer personal data from an unsecured server.
- B. A hacker using a stolen administrator identity alerts the discount percentage in the product database.
- C. A DDoS attack renders the customer's cloud inaccessible for 24 hours.
- D. An administrator inadvertently click on Phish bait exposing his company to a ransomware attack.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 33

To assist an organization with planning a cloud migration strategy to execution, an auditor should recommend the use of:

- A. enterprise architecture.
- B. object-oriented architecture.
- C. service-oriented architecture.
- D. software architecture.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 34

Who is responsible for the security of the physical infrastructure and virtualization platform?

- A. The majority is covered by the consumer
- B. The cloud consumer
- C. The cloud provider
- D. It depends on the agreement

E. The responsibility is split equally

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

To understand their compliance alignments and gaps with a cloud provider, what must cloud customers rely on?

- A. EDiscovery tools
- B. Provider and consumer contracts
- C. Provider documentation
- D. Third-party attestations
- E. Provider run audits and reports

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 36

What is known as a code execution environment running within an operating system that shares and uses the resources of the operating system?

- A. Pod
- B. Platform-based Workload
- C. Container
- D. Abstraction
- E. Virtual machine

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 37

An important consideration when performing a remote vulnerability test of a cloud-based application is to

- A. Schedule vulnerability test at night
- B. Use network layer testing tools exclusively
- C. Use techniques to evade cloud provider's detection systems
- D. Use application layer testing tools exclusively
- E. Obtain provider permission for test

Answer: E ([LEAVE A REPLY](#))

NEW QUESTION: 38

The rapid and dynamic rate of changes found in a cloud environment affects the organization's:

- A. risk scoring.
- B. risk appetite.
- C. risk profile.
- D. risk communication.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 39

During an audit it was identified that a critical application hosted in an off-premises cloud is not part of the organization's DRP (Disaster Recovery Plan). Management stated that it is responsible for ensuring that the cloud service provider (CSP) has a plan that is tested annually. What should be the auditor's NEXT course of action?

- A. Plan an audit of the CSP.
- B. Review the CSP audit reports.
- C. Review the contract and DR capability.
- D. Review the security white paper of the CSP.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 40

Which of the following is a perceived advantage or disadvantage of managing enterprise risk for cloud deployments?

- A. Decreased requirement for proactive management of relationship and adherence to contracts.
- B. More physical control over assets and processes.
- C. Increased need, but reduction in costs, for managing risks accepted by the cloud provider.
- D. None of the above.
- E. Greater reliance on contracts, audits, and assessments due to lack of visibility or management.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 41

Supply chain agreements between CSP and cloud customers should, at minimum, include:

- A. Audits, assessments and independent verification of compliance certifications with agreement terms
- B. Policies and procedures of the cloud customer
- C. Organization chart of the CSP
- D. Regulatory guidelines impacting the cloud customer

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 42

Changes to which of the following will MOST likely influence the expansion or reduction of controls required to remediate the risk arising from changes to an organization's SaaS vendor?

- A. Risk appetite
- B. Risk exceptions policy
- C. Contractual requirements

D. Board oversight

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 43

When deploying Security as a Service in a highly regulated industry or environment, what should both parties agree on in advance and include in the SLA?

- A. The duration of time that a security violation can occur before the client begins assessing regulatory fines.
- B. The regulations that are pertinent to the contract and how to circumvent them.
- C. The type of security software which meets regulations and the number of licenses that will be needed.
- D. The cost per incident for security breaches of regulated information.
- E. The metrics defining the service level required to achieve regulatory objectives.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 44

When applying the Top Threats Analysis methodology following an incident, what is the scope of the technical impact identification step?

- A. Determine the impact on confidentiality, integrity and availability of the information system.
- B. Determine the impact on the controls that were selected by the organization to respond to identified risks.
- C. Determine the impact on the financial, operational, compliance and reputation of the organization.
- D. Determine the impact on the physical and environmental security of the organization, excluding informational assets.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 45

A cloud service provider does not allow audits using automated tools as these tools could be considered destructive techniques for the cloud environment. Which of the following aspects of the audit will be constrained?

- A. Purpose
- B. Objectives
- C. Nature of relationship
- D. Scope

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 46

Which cloud-based service model enables companies to provide client-based access for partners to databases or applications?

- A. Software-as-a-service (SaaS)
- B. Identity-as-a-service (IDaaS)
- C. Desktop-as-a-service (DaaS)
- D. Infrastructure-as-a-service (IaaS)
- E. Platform-as-a-service (PaaS)

Answer: ([SHOW ANSWER](#))

Valid CCAK Dumps shared by BraindumpsPass.com for Helping Passing CCAK Exam! BraindumpsPass.com now offer the **newest CCAK exam dumps**, the BraindumpsPass.com CCAK exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CCAK dumps with Test Engine here: <https://www.braindumpsPASS.com/ISACA/CCAK-practice-exam-dumps.html> (207 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 47

Which of the following is the risk associated with storing data in a cloud that crosses jurisdictions?

- A. Provider administration risk
- B. Audit risk
- C. Compliance risk
- D. Virtualization risk

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 48

During a review, an IS auditor notes that an organization's marketing department has purchased a cloud-based software application without following the procurement process. What should the auditor do FIRST?

- A. Escalate to senior management.
- B. Perform a risk analysis.
- C. Review the business impact analysis (BIA).
- D. Review the procurement process.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 49

Your SLA with your cloudprovider ensures continuity for all services.

- A. True
- B. False

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 50

Which of the following items is NOT an example of Security as a Service (SecaaS)?

- A. Spam filtering
- B. Authentication
- C. Web filtering
- D. Provisioning
- E. Intrusion detection

Answer: (SHOW ANSWER)

NEW QUESTION: 51

Which term is used to describe the use of tools to selectively degrade portions of the cloud to continuously test business continuity?

- A. Organized Downtime
- B. Chaos Engineering
- C. Planned Outages
- D. Expected Engineering
- E. Resiliency Planning

Answer: B (LEAVE A REPLY)

NEW QUESTION: 52

Which of the following attestation allows for immediate adoption of the Cloud Control Matrix (CCM) as additional criteria to AICPA Trust Service Criteria and provides the flexibility to update the criteria as technology and market requirements change?

- A. PC-IDSS
- B. MTCS
- C. BSI Criteria Catalogue C5
- D. CSA STAR Attestation

Answer: D (LEAVE A REPLY)

NEW QUESTION: 53

What is resource pooling?

- A. Internet-based CPUs are pooled to enable multi-threading.
- B. The provider's computing resources are pooled to serve multiple consumers.
- C. The dedicated computing resources of each client are pooled together in a colocation facility.
- D. None of the above.
- E. Placing Internet ("cloud") data centers near multiple sources of energy, such as hydroelectric dams.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 54

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

- A. Identification of roles and responsibilities
- B. Identification of processes, functions, and systems
- C. Identification of the relevant laws, regulations, and standards
- D. Development of the monitoring goals and requirements

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 55

Which of the following cloud deployment models would BEST meet the needs of a startup software development organization with limited initial capital?

- A. Community
- B. Private
- C. Hybrid
- D. Public

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 56

When migrating to a cloud environment, which of the following should be the PRIMARY driver for the use of encryption?

- A. Organizational security policies
- B. Cost-benefit analysis
- C. The presence of PII
- D. Cloud Service Provider encryption capabilities

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 57

What is true of companies considering a cloud computing business relationship?

- A. The companies using the cloud providers are the custodians of the data entrusted to them.
- B. The cloud computing companies are absolved of all data security and associated risks through contracts and data laws.
- C. The laws protecting customer data are based on the cloud provider and customer location only.
- D. The cloud computing companies own all customer data.
- E. The confidentiality agreements between companies using cloud computing services is limited legally to the company, not the provider.

Answer: A ([LEAVE A REPLY](#))

Valid CCAK Dumps shared by BraindumpsPass.com for Helping Passing CCAK Exam! BraindumpsPass.com now offer the **newest CCAK exam dumps**, the BraindumpsPass.com CCAK exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CCAK dumps with Test Engine here: <https://www.braindumpsPass.com/ISACA/CCAK-practice-exam-dumps.html> (207 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)