

[Feb-2023 Pass ISACA CCAK Tests Engine pdf - All Free Dumps [Q67-Q88]



[Feb-2023] Pass ISACA CCAK Tests Engine pdf - All Free Dumps [Q67-Q88]

[Feb-2023] Pass ISACA CCAK Tests Engine pdf - All Free Dumps
Certificate of Cloud Auditing Knowledge Practice Tests 2023 | Pass CCAK with confidence!

QUESTION 67

Your cloud and on-premises infrastructures should always use the same network address ranges.

- * False
- * True

QUESTION 68

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

- * Obtain provider permission for test
- * Use techniques to evade cloud provider's detection systems
- * Use application layer testing tools exclusively
- * Use network layer testing tools exclusively
- * Schedule vulnerability test at night

QUESTION 69

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

- * Community
- * Public
- * Hybrid
- * Private

QUESTION 70

An organization has an ISMS implemented, following ISO 27001 and Annex A controls. The CIO would like to migrate some of the infrastructure to the cloud. Which of the following standards would BEST assist in identifying controls to consider for this migration?

- * ISO/IEC 27701
- * ISO/IEC 22301
- * ISO/IEC 27002
- * ISO/IEC 27017

Explanation

ISO/IEC 27017 standard defines the requirements for an information security management system (ISMS).

Note that the entire organization is not necessarily affected by the standard, because it all depends on the scope of the ISMS. The scope could be limited by the provider to one group within an organization, and there is no guarantee that any group outside of the scope has appropriate ISMSs in place. It is up to the auditor to verify that the scope of the engagement is fit for purpose. As the customer, you are responsible for determining whether the scope of the certification is relevant for your purposes.

QUESTION 71

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

- * Cloud Service Provider encryption capabilities
- * The presence of PII
- * Organizational security policies
- * Cost-benefit analysis

QUESTION 72

Which of the following metrics are frequently immature?

- * Metrics around Infrastructure as a Service (IaaS) storage and network environments
- * Metrics around Platform as a Service (PaaS) development environments
- * Metrics around Infrastructure as a Service (IaaS) computing environments
- * Metrics around specific Software as a Service (SaaS) application services

QUESTION 73

The Cloud Octagon Model was developed to support organizations:

- * risk assessment methodology.
- * risk treatment methodology.
- * incident response methodology.

- * incident detection methodology.

QUESTION 74

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

- * Design
- * Stakeholder identification
- * Development
- * Risk assessment

QUESTION 75

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

- * Policy based access control
- * Attribute based access control
- * Rule based access control
- * Role based access control

QUESTION 76

Which of the following is the MOST feasible way to validate the performance of CSPs for the delivery of technology resources?

- * Cloud compliance program
- * Legacy IT compliance program
- * Internal audit program
- * Service organization controls report

QUESTION 77

Which of the following are the three MAIN phases of the cloud controls matrix (CCM) mapping methodology?

- * Plan –> Develop –> Release
- * Deploy –> Monitor –> Audit
- * Initiation –> Execution –> Monitoring and Controlling
- * Preparation –> Execution –> Peer Review and Publication

QUESTION 78

Which statement best describes why it is important to know how data is being accessed?

- * The devices used to access data have different storage formats.
- * The devices used to access data use a variety of operating systems and may have different programs installed on them.
- * The device may affect data dispersion.
- * The devices used to access data use a variety of applications or clients and may have different security characteristics.
- * The devices used to access data may have different ownership characteristics.

QUESTION 79

Which statement about compliance responsibilities and ownership of accountability is correct?

- * Organizations may be able to transfer their accountability for compliance with various regulatory requirements to their CSPs, but they retain the ownership of responsibility.
- * Organizations may be able to transfer their responsibility for compliance with various regulatory requirements to their CSPs, but they retain the ownership of accountability.

- * Organizations may transfer their responsibility and accountability for compliance with various regulatory requirements to their CSPs.
- * Organizations are not able to transfer their responsibility nor accountability for compliance with various regulatory requirements to their CSPs.

QUESTION 80

A third-party service provider is hosting a private cloud for an organization. Which of the following findings during an audit of the provider poses the GREATEST risk to the organization?

- * 2% of backups had to be rescheduled due to backup media failures.
- * The organization's virtual machines share the same hypervisor with virtual machines of other clients.
- * Two different hypervisor versions are used due to the compatibility restrictions of some virtual machines.
- * 5% of detected incidents exceeded the defined service level agreement (SLA) for escalation.

QUESTION 81

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

- * The hypervisor
- * Virtualization management components apart from the hypervisor
- * Configuration and VM sprawl issues
- * All of the above

QUESTION 82

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?

- * Risk exceptions policy
- * Contractual requirements
- * Risk appetite
- * Board oversight

QUESTION 83

What factors should you understand about the data specifically due to legal, regulatory, and jurisdictional factors?

- * The physical location of the data and how it is accessed
- * The fragmentation and encryption algorithms employed
- * The language of the data and how it affects the user
- * The implications of storing complex information on simple storage systems
- * The actual size of the data and the storage format

QUESTION 84

A Dot Release of Cloud Control Matrix (CCM) indicates what?

- * The introduction of new control frameworks mapped to previously-published CCM controls.
- * A revision of the CCM domain structure.
- * A technical change (revision or addition or deletion) of a number of controls is smaller than 10% compared to the previous Full release.
- * A technical change (revision or addition or deletion) of a number of controls is greater than 10% compared to the previous Full release.

QUESTION 85

Which of the following is a cloud-specific security standard?

- * ISO27017
- * ISO27701
- * ISO22301
- * ISO14001

QUESTION 86

ENISA: VMhopping is:

- * Improper management of VM instances, causing customer VMs to be commingled with other customer systems.
- * Looping within virtualized routing systems.
- * Lack of vulnerability management standards.
- * Using a compromised VM to exploit a hypervisor, used to take control of other VMs.
- * Instability in VM patch management causing VM routing errors.

QUESTION 87

An organization has an ISMS implemented, following ISO 27001 and Annex A controls. The CIO would like to migrate some of the infrastructure to the cloud. Which of the following standards would BEST assist in identifying controls to consider for this migration?

- * ISO/IEC 27701
- * ISO/IEC 22301
- * ISO/IEC 27002
- * ISO/IEC 27017

ISO/IEC 27017 standard defines the requirements for an information security management system (ISMS). Note that the entire organization is not necessarily affected by the standard, because it all depends on the scope of the ISMS. The scope could be limited by the provider to one group within an organization, and there is no guarantee that any group outside of the scope has appropriate ISMSs in place. It is up to the auditor to verify that the scope of the engagement is fit for purpose. As the customer, you are responsible for determining whether the scope of the certification is relevant for your purposes.

QUESTION 88

What data center and physical security measures should a cloud customer consider when assessing a cloud service provider?

- * Assess use of monitoring systems to control ingress and egress points of entry to the data center.
- * Implement physical security perimeters to safeguard personnel, data and information systems.
- * Conduct a due diligence to verify the cloud provider applies adequate physical security measures.
- * Review internal policies and procedures for relocation of hardware and software to an offsite location.

Online Exam Practice Tests with detailed explanations!: <https://www.actualtests4sure.com/CCAK-test-questions.html>