Ultimate Guide to Prepare CCAK Certification Exam for Cloud Security Alliance in 2022 [Q39-Q60

Ultimate Guide to Prepare CCAK Certification Exam for Cloud Security Alliance in 2022
Use Real CCAK Dumps - ISACA Correct Answers updated on 2022

ISACA CCAK Exam Syllabus Topics:

TopicDetailsTopic 1- Continuous Assurance and Compliance- Cloud Compliance ProgramTopic 2- Evaluating a Cloud Compliance Program- Cloud AuditingTopic 3- CCM and CAIQ: Goals, Objectives, and Structure- CCM: Auditing ControlsTopic 4- A Threat Analysis Methodology for Cloud Using CCM- Cloud Governance

NO.39 In the context of Infrastructure as a Service (IaaS), a vulnerability assessment will scan virtual machines to identify vulnerabilities in:

* both operating system and application infrastructure contained within the CSP’s instances.
* both operating system and application infrastructure contained within the customer’s instances
* only application infrastructure contained within the CSP’s instances.
* only application infrastructure contained within the customer’s instances.

NO.40 As a developer building codes into a container in a DevSecOps environment, which of the following is the appropriate place(s) to perform security tests?
* Within developer’s laptop
* Within the CI/CD server
* Within version repositories
* Within the CI/CD pipeline

NO.41 If the degree of verification for information shared with the auditor during an audit is low, the auditor should:
* reject the information as audit evidence.
* stop evaluating the requirement altogether and review other audit areas.
* delve deeper to obtain the required information to decide conclusively.
* use professional judgment to determine the degree of reliance that can be placed on the information as evidence.

NO.42 CCM: The following list of controls belong to which domain of the CCM?

GRM 06 – Policy GRM 07- Policy Enforcement GRM 08 – Policy Impact on Risk Assessments GRM 09 – Policy Reviews GRM 10 – Risk Assessments GRM 11 – Risk Management Framework
* Governance and Retention Management
* Governance and Risk Management
* Governing and Risk Metrics

NO.43 With regard to the Cloud Control Matrix (CCM), the ‘Architectural Relevance’ is a feature that enables the filtering of security controls by:
* relevant architecture frameworks such as the NIST Enterprise Architecture Model, the Federal Enterprise Architecture Framework (FEAF), The Open Group Architecture Framework (TOGAF), and the Zachman Framework for Enterprise Architecture.
* relevant delivery models such as Software as a Service, Platform as a Service, Infrastructure as a Service.
* relevant architectural paradigms such as Client-Server, Mainframe, Peer-to-Peer, and SmartClient-Backend.
* relevant architectural components such as Physical, Network, Compute, Storage, Application, and Data.

NO.44 Which of the following should be an IS auditor’s GREATEST concern when reviewing an outsourcing arrangement with a third-party cloud service provider to host personally identifiable data?
* The data is not adequately segregated on the host platform.
* Fees are charged based on the volume of data stored by the host.
* The outsourcing contract does not contain a right-to-audit clause.
* The organization’s servers are not compatible with the third party’s infrastructure

NO.45 Segregation of duties would be compromised if:
* application programmers moved programs into production.
* application programmers accessed test data.
* database administrators (DBAs) modified the structure of user tables.
* operations staff modified batch schedules.

NO.46 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

NO.47 Which of the following approaches encompasses social engineering of staff, bypassing of physical access controls and

penetration testing?
* Blue team
* White box
* Gray box
* Red team

NO.48 Which of the following is the BEST way for a client to enforce a policy violation committed by a cloud service provider (CSP)?
* The violation is agreed upon and documented.
* Nothing can be done to enforce violations as this is a cloud service.
* The violation is agreed to verbally by the CSP.
* Violations will be automatically enforced so no action is needed.

NO.49 Which of the following is an example of a corrective control?
* A central anti-virus system installing the latest signature files before allowing a connection to the network
* Unsuccessful access attempts being automatically logged for investigation
* Privileged access to critical information systems requiring a second factor of authentication using soft token
* All new employees having standard access rights until their manager approves privileged rights

NO.50 Which statement best describes the impact of Cloud Computing on business continuity management?
* A general lack of interoperability standards means that extra focus must be placed on the security aspects of migration between Cloud providers.
* The size of data sets hosted at a Cloud provider can present challenges if migration to another provider becomesnecessary.
* Customers of SaaS providers in particular need to mitigate the risks of application lock-in.
* Clients need to do business continuity planning due diligence in case they suddenly need to switch providers.
* Geographic redundancyensures that Cloud Providers provide highly available services.

NO.51 An auditor is performing an audit on behalf of a cloud customer. For assessing security awareness, the auditor should:
* assess the existence and adequacy of a security awareness training program at the cloud service provider’s organization as the cloud customer hired the auditor to review and cloud service.
* assess the existence and adequacy of a security awareness training program at both the cloud customer’s organization and the cloud service provider’s organization.
* assess the existence and adequacy of a security awareness training program at the cloud customer’s organization as they hired the auditor.
* not assess the security awareness training program as it is each organization’s responsibility

NO.52 Which governance domain deals with evaluating how cloudcomputing affects compliance with internal security policies and various legal requirements, such as regulatory and legislative?
* Legal Issues: Contracts and Electronic Discovery
* Infrastructure Security
* Compliance and Audit Management
* Information Governance
* Governance and Enterprise Risk Management

NO.53 The criteria for limiting services allowing non-critical services or services requiring high availability and resilience to be moved to the cloud is an important consideration to be included PRIMARILY in the:
* risk management policy.
* cloud policy.
* business continuity plan.
* information security standard for cloud technologies.

NO.54 An IS auditor is a member of an application development team that is selecting software. Which of the following would impair the auditor’s independence?
* Approving the vendor selection methodology
* verifying the weighting of each selection criteria
* Reviewing the request for proposal (RFP)
* Witnessing the vendor selection process

NO.55 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

NO.56 How does running applications on distinct virtual networks and only connecting networksas needed help?
* It reduces hardware costs
* It provides dynamic and granular policies with less management overhead
* It locks down access and provides stronger data security
* It reduces the blast radius of a compromised system
* It enables you to configure applications around business groups

NO.57 When establishing cloud governance, an organization should FIRST test by migrating:
* all applications at once to the cloud.
* complex applications to the cloud.
* legacy applications to the cloud.
* a few applications to the cloud.

NO.58 Which of the following standards is designed to be used by organizations for cloud services that intend to select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001?
* ISO/IEC 27017:2015
* CSA Cloud Control Matrix (CCM)
* NIST SP 800-146
* ISO/IEC 27002

NO.59 What is a sign of an organization that has adopted a shift-left concept of code release cycles?
* A waterfall model to move resources through the development to release phases
* Incorporation of automation to identify and address software code problems early
* Maturity of start-up entities with high-iteration to low-volume code commits
* Large entities with slower release cadences and geographical dispersed systems

NO.60 When performing audits in relation to Business Continuity Management and Operational Resilience strategy, what would be the MOST critical aspect to audit in relation to the strategy of the cloud customer that should be formulated jointly with the cloud service provider?
* Validate if the strategy covers unavailability of all components required to operate the business-as-usual or in disrupted mode, in parts or total- when impacted by a disruption.
* Validate if the strategy covers all aspects of Business Continuity and Resilience planning, taking inputs from the assessed impact and risks, to consider activities for before, during, and after a disruption.
* Validate if the strategy covers all activities required to continue and recover prioritized activities within identified time frames and agreed capacity, aligned to the risk appetite of the organization including the invocation of continuity plans and crisis management capabilities.

* Validate if the strategy is developed by both cloud service providers and cloud service consumers within the acceptable limits of their risk appetite.

Cloud Security Alliance -CCAK Exam-Practice-Dumps: https://www.actualtests4sure.com/CCAK-test-questions.html]