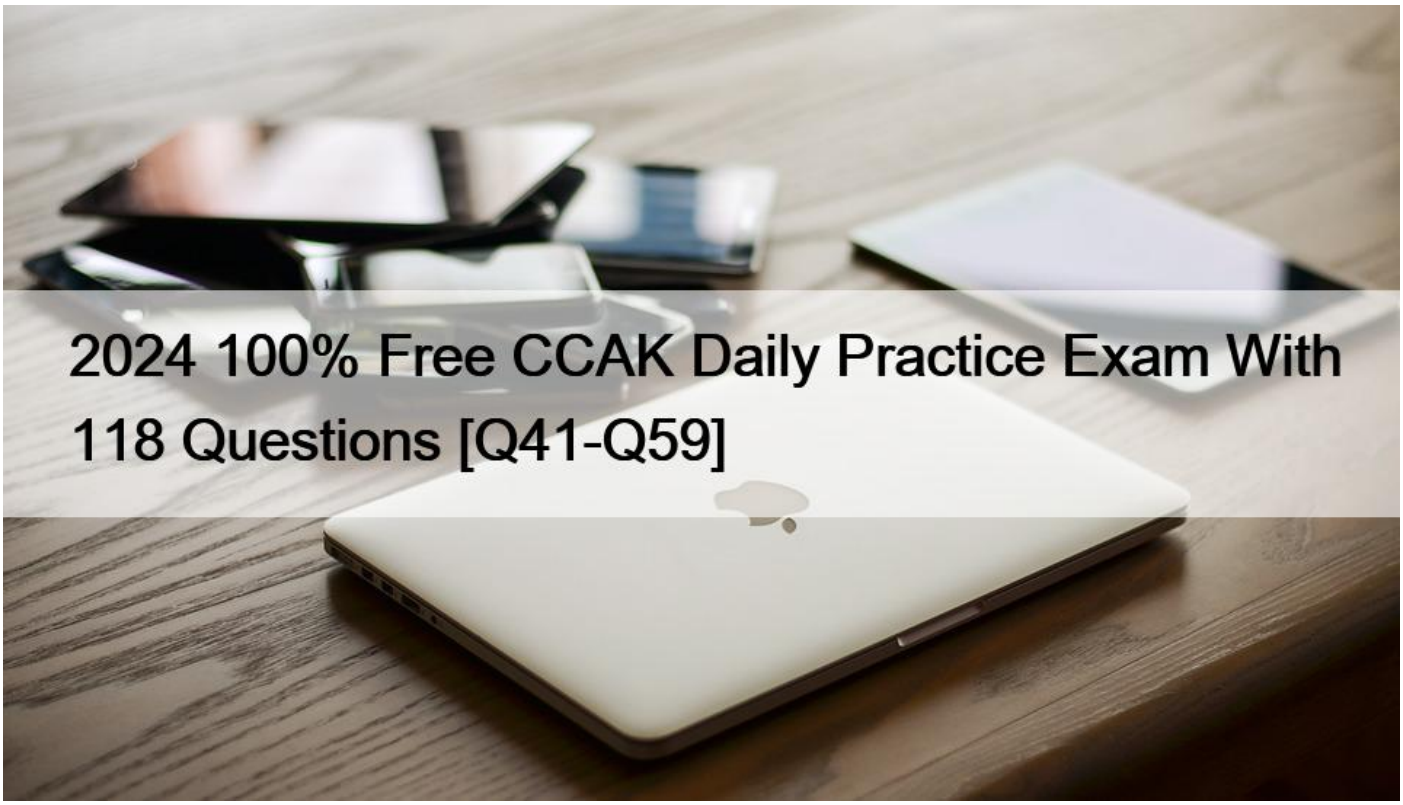
2024 100% Free CCAK Daily Practice Exam With 118 Questions [Q41-Q59



2024 100% Free CCAK Daily Practice Exam With 118 Questions
CCAK exam torrent ISACA study guide

The CCAK Certification Exam is the first of its kind in the industry, and was developed by ISACA (Information Systems Audit and Control Association), a global organization that provides education, certification, and advocacy for cybersecurity and IT governance professionals. CCAK exam covers a range of cloud computing topics, including cloud service models, security and privacy, risk management, compliance, and more.

NEW QUESTION 41

Which of the following is the PRIMARY area for an auditor to examine in order to understand the criticality of the cloud services in an organization, along with their dependencies and risks?
* Contractual documents of the cloud service provider
* Heat maps
* Data security process flow
* Turtle diagram
Explanation

Heat maps are graphical representations of data that use color-coding to show the relative intensity, frequency, or magnitude of a

variable1. Heat maps can be used to visualize the criticality of the cloud services in an organization, along with their dependencies and risks, by mapping the cloud services to different dimensions, such as business impact, availability, security, performance, cost, etc. Heat maps can help auditors identify the most important or vulnerable cloud services, as well as the relationships and trade-offs among them2.

For example, Azure Charts provides heat maps for various aspects of Azure cloud services, such as updates, trends, pillars, areas, geos, categories, etc3. These heat maps can help auditors understand the current state and dynamics of Azure cloud services and compare them across different dimensions4.

Contractual documents of the cloud service provider are the legal agreements that define the terms and conditions of the cloud service, including the roles, responsibilities, and obligations of the parties involved.

They may provide some information on the criticality of the cloud services in an organization, but they are not as visual or comprehensive as heat maps. Data security process flow is a diagram that shows the steps and activities involved in protecting data from unauthorized access, use, modification, or disclosure. It may help auditors understand the data security controls and risks of the cloud services in an organization, but it does not cover other aspects of criticality, such as business impact or performance. Turtle diagram is a tool that helps analyze a process by showing its inputs, outputs, resources, criteria, methods, and interactions. It may help auditors understand the process flow and dependencies of the cloud services in an organization, but it does not show the relative importance or risks of each process element.

References:

What is a Heat Map? Definition from WhatIs.com1, section on Heat Map

Cloud Computing Security Considerations | Cyber.gov.au2, section on Cloud service criticality Azure Charts – Clarity for the Cloud3, section on Heat Maps Azure Services Overview4, section on Heat Maps Cloud Services Due Diligence Checklist | Trust Center, section on How to use the checklist Data Security Process Flow – an overview | ScienceDirect Topics, section on Data Security Process Flow What is a Turtle Diagram? Definition from WhatIs.com, section on Turtle Diagram

NEW QUESTION 42

CCM: In the CCM tool, “Encryption and Key Management” is an example of which of the following?
* Risk Impact
* Domain
* Control Specification

NEW QUESTION 43

Which of the following has been provided by the Federal Office for Information Security in Germany to support customers in selecting, controlling, and monitoring their cloud service providers?
* BSI IT-basic protection catalogue
* Multi-Tier Cloud Security (MTCS)
* German IDW PS 951
* BSI Criteria Catalogue C5

Explanation

The BSI Criteria Catalogue C5 is a document that has been provided by the Federal Office for Information Security (BSI) in Germany to support customers in selecting, controlling, and monitoring their cloud service providers (CSPs). The C5 stands for Cloud Computing Compliance Criteria Catalogue and specifies minimum requirements for secure cloud computing. The C5 is primarily intended for professional CSPs, their auditors, and customers of the CSPs. The C5 covers 17 domains and 114 control

objectives that address all key aspects of cloud security, such as data protection, identity and access management, encryption and key management, incident response, audit assurance, and compliance. The C5 also maps to other industry-accepted security standards, regulations, and frameworks, such as ISO 27001/27002/27017/27018, NIST SP 800-53, CSA Cloud Controls Matrix (CCM), COBIT, GDPR, etc. The C5 helps customers to evaluate and compare the security and compliance posture of different CSPs, and to verify that the CSPs meet their contractual obligations and legal requirements12.

References:

BSI – C5 criteria catalogue – Federal Office for Information Security

Germany C5 – Azure Compliance | Microsoft Learn

NEW QUESTION 44

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

NEW QUESTION 45

SAST testing is performed by:
* scanning the application source code.
* scanning the application interface.
* scanning all infrastructure components.
* performing manual actions to gain control of the application.

SAST analyzes application code offline. SAST is generally a rules-based test that will scan software code for items such as credentials embedded into application code and a test of input validation, both of which are major concerns for application security.

NEW QUESTION 46

A new company has all its operations in the cloud. Which of the following would be the BEST information security control framework to implement?
* NIST 800-73, because it is a control framework implemented by the main cloud providers
* ISO/IEC 27018
* ISO/IEC 27002
* (S) Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

Explanation

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) would be the best information security control framework to implement for a new company that has all its operations in the cloud. The CCM is a cybersecurity control framework for cloud computing that is aligned to the CSA best practices and is considered the de-facto standard for cloud security and privacy. The CCM covers 17 domains and 197 control objectives that address all key aspects of cloud technology, such as data security, identity and access management, encryption and key management, incident response, audit assurance, and compliance. The CCM also maps to other industry-accepted security standards, regulations, and frameworks, such as ISO

27001/27002/27017/27018, NIST SP 800-53, PCI DSS, COBIT, FedRAMP, etc., which can help the company to achieve multiple compliance goals with one framework. The CCM also provides guidance on the shared responsibility model between cloud service

providers and cloud customers, and helps to define the organizational relevance of each control12.

References:

Cloud Controls Matrix (CCM) – CSA

Cloud Controls Matrix and CAIQ v4 | CSA – Cloud Security Alliance

NEW QUESTION 47

To ensure a cloud service provider is complying with an organization’s privacy requirements, a cloud auditor should FIRST review:
* organizational policies, standards, and procedures.
* adherence to organization policies, standards, and procedures.
* legal and regulatory requirements.
* the IT infrastructure.

Explanation

To ensure a cloud service provider is complying with an organization’s privacy requirements, a cloud auditor should first review the organizational policies, standards, and procedures that define the privacy objectives, expectations, and responsibilities of the organization. The organizational policies, standards, and procedures should also reflect the legal and regulatory requirements that apply to the organization and its cloud service provider, as well as the best practices and guidelines for cloud privacy. The organizational policies, standards, and procedures should provide the basis for evaluating the cloud service provider’s privacy practices and controls, as well as the contractual terms and conditions that govern the cloud service agreement. The cloud auditor should compare the organizational policies, standards, and procedures with the cloud service provider’s self-disclosure statements, third-party audit reports, certifications, attestations, or other evidence of compliance123.

Reviewing the adherence to organization policies, standards, and procedures (B) is a subsequent step that the cloud auditor should perform after reviewing the organizational policies, standards, and procedures themselves. The cloud auditor should assess whether the cloud service provider is following the organization’s policies, standards, and procedures consistently and effectively, as well as whether the organization is monitoring and enforcing the compliance of the cloud service provider. The cloud auditor should also identify any gaps or deviations between the organization’s policies, standards, and procedures and the actual practices and controls of the cloud service provider123.

Reviewing the legal and regulatory requirements is an important aspect of ensuring a cloud service provider is complying with an organization’s privacy requirements, but it is not the first step that a cloud auditor should take. The legal and regulatory requirements may vary depending on the jurisdiction, industry, or sector of the organization and its cloud service provider. The legal and regulatory requirements may also change over time or be subject to interpretation or dispute. Therefore, the cloud auditor should first review the organizational policies, standards, and procedures that incorporate and translate the legal and regulatory requirements into specific and measurable privacy objectives, expectations, and responsibilities for both parties123.

Reviewing the IT infrastructure (D) is not a relevant or sufficient step for ensuring a cloud service provider is complying with an organization’s privacy requirements. The IT infrastructure refers to the hardware, software, network, and other components that support the delivery of cloud services. The IT infrastructure is only one aspect of cloud security and privacy, and it may not be accessible or visible to the cloud auditor or the organization. The cloud auditor should focus on reviewing the privacy practices and controls that are implemented by the cloud service provider at different layers of the cloud service model (IaaS, PaaS, SaaS), as well as the contractual terms and conditions that define the privacy rights and obligations of both parties123.

References :=

Cloud Audits and Compliance: What You Need To Know – Linford & Company LLP Trust in the Cloud in audits of cloud services – PwC Cloud Compliance & Regulations Resources | Google Cloud

NEW QUESTION 48

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.

NEW QUESTION 49

Which of the following is the MOST significant difference between a cloud risk management program and a traditional risk management program?
* Virtualization of the IT landscape
* Shared responsibility model
* Risk management practices adopted by the cloud service provider
* Hosting sensitive information in the cloud environment

Explanation

The most significant difference between a cloud risk management program and a traditional risk management program is the shared responsibility model. The shared responsibility model is the division of security and compliance responsibilities between the cloud service provider and the cloud service customer, depending on the type of cloud service model (IaaS, PaaS, SaaS). The shared responsibility model implies that both parties have to collaborate and coordinate to ensure that the cloud service meets the required level of security and compliance, as well as to identify and mitigate any risks that may arise from the cloud environment123.

Virtualization of the IT landscape (A) is a difference between a cloud risk management program and a traditional risk management program, but it is not the most significant one. Virtualization of the IT landscape refers to the abstraction of physical IT resources, such as servers, storage, network, or applications, into virtual ones that can be accessed and managed over the internet. Virtualization of the IT landscape enables the cloud service provider to offer scalable, flexible, and efficient cloud services to the cloud service customer. However, virtualization of the IT landscape also introduces new risks, such as data leakage, unauthorized access, misconfiguration, or performance degradation123.

Risk management practices adopted by the cloud service provider are a difference between a cloud risk management program and a traditional risk management program, but they are not the most significant one.

Risk management practices adopted by the cloud service provider refer to the methods or techniques that the cloud service provider uses to identify, assess, treat, monitor, and report on the risks that affect their cloud services. Risk management practices adopted by the cloud service provider may include policies, standards, procedures, controls, audits, certifications, or attestations that demonstrate their security and compliance posture. However, risk management practices adopted by the cloud service provider are not sufficient or reliable on their own, as they may not cover all aspects of cloud security and compliance, or may not align with the expectations or requirements of the cloud service customer123.

Hosting sensitive information in the cloud environment (D) is a difference between a cloud risk management program and a traditional risk management program, but it is not the most significant one. Hosting sensitive information in the cloud environment refers to storing or processing data that are confidential, personal, or valuable in the cloud infrastructure or platform that is owned and operated by the cloud service provider.

Hosting sensitive information in the cloud environment can offer benefits such as cost savings, accessibility, availability, or backup. However, hosting sensitive information in the cloud environment also poses risks such as data breaches, privacy violations, compliance failures, or legal disputes123. References := Cloud Risk Management – ISACA Cloud Risk Management: A Primer for Security Professionals – Infosec …

Cloud Risk Management: A Primer for Security Professionals – Infosec …

NEW QUESTION 50

Organizations maintain mappings between the different control frameworks they adopt to:
* help identify controls with common assessment status.
* avoid duplication of work when assessing compliance,
* help identify controls with different assessment status.
* start a compliance assessment using the latest assessment.

Explanation

Organizations maintain mappings between the different control frameworks they adopt to avoid duplication of work when assessing compliance. This is because different control frameworks may have overlapping or equivalent controls that address the same objectives or risks. By mapping these controls, organizations can streamline their compliance assessment process and reduce the cost and effort involved. Mappings also help organizations to identify any gaps or inconsistencies in their control coverage and address them accordingly. This is part of the Cloud Control Matrix (CCM) domain COM-03: Control Frameworks, which states that “The organization should identify and adopt applicable control frameworks, standards, and best practices to support the cloud compliance program.”1 References := CCAK Study Guide, Chapter 3: Cloud Compliance Program, page 54

NEW QUESTION 51

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.

NEW QUESTION 52

In relation to testing business continuity management and operational resilience, an auditor should review which of the following database documentation?
* Database backup and replication guidelines
* System backup documentation
* Incident management documentation
* Operational manuals

Explanation

Database backup and replication guidelines are essential for ensuring the availability and integrity of data in the event of a disruption or disaster. They describe how the data is backed up, stored, restored, and synchronized across different locations and platforms. An auditor should review these guidelines to verify that they are aligned with the business continuity objectives, policies, and procedures of the organization and the cloud service provider. The auditor should also check that the backup and replication processes are tested regularly and that the results are documented and reported. References:

ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 96 Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM) v4.0, 2021, BCR-01: Business Continuity Planning/Resilience

NEW QUESTION 53

An organization that is utilizing a community cloud is contracting an auditor to conduct a review on behalf of the group of organizations within the cloud community. From the following, to whom should the auditor report the findings?
* Public
* Management of organization being audited
* Shareholders/interested parties
* Cloud service provider

NEW QUESTION 54

Within an organization, which of the following functions should be responsible for defining the cloud adoption approach?
* Audit committee
* Compliance manager
* IT manager
* Senior management

NEW QUESTION 55

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?
* ISAE 3402 report
* ISO/IEC 27001 certification
* SOC1 Type 1 report
* SOC2 Type 2 report

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.12 References := CCAK Study Guide, Chapter 5: Cloud Auditing, page 971; SOC 2 Type II Compliance: Definition, Requirements, and Why You Need It2

NEW QUESTION 56

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?
* Double gray box
* Tandem
* Reversal
* Double blind

NEW QUESTION 57

What should be an organization’s control audit schedule of a cloud service provider’s business continuity plan and

operational resilience policy?
* Annual
* Quarterly
* Monthly
* Semi-annual

NEW QUESTION 58

The PRIMARY objective for an auditor to understand the organization’s context for a cloud audit is to:
* determine whether the organization has carried out control self-assessment and validated audit reports of the cloud service providers (CSP).
* validate an understanding of the organization’s current state and how the cloud audit plan fits into the existing audit approach.
* validate whether an organization has a cloud audit plan in place.
* validate the organization’s performance effectiveness utilizing cloud service providers (CSP) solutions.

NEW QUESTION 59

What is a sign that an organization has adopted a shift-left concept of code release cycles?
* Large entities with slower release cadences and geographically dispersed systems
* Incorporation of automation to identify and address software code problems early
* A waterfall model remove resources through the development to release phases
* Maturity of start-up entities with high-iteration to low-volume code commits
Explanation

The shift-left concept of code release cycles is a practice that aims to integrate testing, quality, and performance evaluation early in the software development life cycle, often before any code is written. This helps to find and prevent defects, improve quality, and enable faster delivery of secure software. One of the key aspects of the shift-left concept is the incorporation of automation to identify and address software code problems early, such as using continuous integration, continuous delivery, and continuous testing tools. Automation can help reduce manual errors, speed up feedback loops, and increase efficiency and reliability123 The other options are not correct because:

Option A is not correct because large entities with slower release cadences and geographically dispersed systems are more likely to face challenges in adopting the shift-left concept, as they may have more complex and legacy systems, dependencies, and processes that hinder agility and collaboration. The shift-left concept requires a culture of continuous improvement, experimentation, and learning that may not be compatible with traditional or siloed organizations4 Option C is not correct because a waterfall model is the opposite of the shift-left concept, as it involves sequential phases of development, testing, and deployment that are performed late in the software development life cycle. A waterfall model does not allow for early detection and correction of defects, feedback, or changes, and can result in higher costs, delays, and risks5 Option D is not correct because maturity of start-up entities with high-iteration to low-volume code commits is not a sign of the shift-left concept, but rather a sign of the agile or lean software development methodologies. These methodologies focus on delivering value to customers by delivering working software in short iterations or sprints, with frequent feedback and adaptation. While these methodologies can support the shift-left concept by enabling faster testing and delivery cycles, they are not equivalent or synonymous with it6 References: 1: AWS. What is DevSecOps? – Developer Security Operations Explained – AWS.

[Online]. Available: 4. [Accessed: 14-Apr-2023]. 2: Dynatrace. Shift left vs shift right: A DevOps mystery solved – Dynatrace news. [Online]. Available: 2. [Accessed: 14-Apr-2023]. 3: BMC Software. Shift Left Testing: What, Why & How To Shift Left – BMC Software | Blogs. [Online]. Available: 3. [Accessed:

14-Apr-2023]. 4: GitLab. How to shift left with continuous integration | GitLab.

[Online]. Available: 4. [Accessed: 14-Apr-2023]. 5: DZone. DevOps and The Shift-Left Principle – DZone.

[Online]. Available: 5. [Accessed: 14-Apr-2023]. 6: Devopedia. Shift Left – Devopedia. [Online]. Available: 6.

[Accessed: 14-Apr-2023].