Try Free and Start Using Realistic Verified CCAK Dumps Instantly [Q21-Q38

Try Free and Start Using Realistic Verified CCAK Dumps Instantly CCAK Actual Questions - Instant Download 207 Questions NO.21 Which of the following is NOT a cloud computing characteristic that impacts incidence response?

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

NO.22 Which of the following is the BEST tool to perform cloud security control audits?

* Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
* General Data Protection Regulation (GDPR)
* Federal Information Processing Standard (FIPS) 140-2
* ISO 27001

The CSA Cloud Controls Matrix (CCM) is the best tool to perform cloud security control audits, as it 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 privacy1. The CCM provides a set of 197 control objectives that are structured in 17 domains covering all key aspects of cloud technology, such as identity and access management, data security, encryption and key management, business continuity and disaster recovery, audit assurance and compliance, and risk management1. The CCM also maps the controls to various industry-accepted security standards, regulations, and control frameworks, such as ISO 27001/27002/27017/27018, NIST SP

800-53, PCI DSS, GDPR, and others1. The CCM can be used as a tool for the systematic assessment of a cloud implementation, and provides guidance on which security controls should be implemented by which actor within the cloud supply chain1. The CCM also includes the Consensus Assessment Initiative Questionnaire (CAIQ), which provides a set of “yes or no” questions based on the security controls in the CCM that can be used to assess a cloud service provider2.

The other options are not the best tools to perform cloud security control audits, as they are either not specific to cloud computing or not comprehensive enough. GDPR is a regulation that aims to protect the personal data and privacy of individuals in the European Union and the European Economic Area3, but it does not provide a framework for cloud security controls. FIPS 140-2 is a standard that specifies the security requirements for cryptographic modules used by federal agencies in the United States, but it does not cover other aspects of cloud security. ISO 27001 is a standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization, but it does not provide specific guidance for cloud services. Reference:

Cloud Controls Matrix (CCM) – CSA

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

General Data Protection Regulation – Wikipedia

[FIPS 140-2 – Wikipedia]

[ISO/IEC 27001:2013]

NO.23 Your cloud and on-premisesinfrastructures should always use the same network address ranges.
* False
* True

NO.24 A CSP providing cloud services currently being used by the United States federal government should obtain which of the following to assure compliance to stringent government standards?
* Multi-Tier Cloud Security (MTCS) Attestation
* FedRAMP Authorization
* ISO/IEC 27001:2013 Certification
* CSA STAR Level Certificate

NO.25 Which of the following provides the BEST evidence that a cloud service provider’s continuous integration and continuous delivery (CI/CD) development pipeline includes checks for compliance as new features are added to its Software as a Service (SaaS) applications?
* Compliance tests are automated and integrated within the Cl tool.
* Developers keep credentials outside the code base and in a secure repository.
* Frequent compliance checks are performed for development environments.
* Third-party security libraries are continuously kept up to date.

A centralized risk and controls dashboard is the best option for ensuring a coordinated approach to risk and control processes when duties are split between an organization and its cloud service providers. This dashboard provides a unified view of risk and control status across the organization and the cloud services it utilizes. It enables both parties to monitor and manage risks effectively and ensures that control activities are aligned and consistent. This approach supports proactive risk management and facilitates communication and collaboration between the organization and the cloud service provider.

References = The concept of a centralized risk and controls dashboard is supported by the Cloud Security Alliance (CSA) and ISACA, which emphasize the importance of visibility and coordination in cloud risk management. The CCAK materials and the Cloud Controls Matrix (CCM) provide guidance on establishing such dashboards as a means to manage and mitigate risks in a cloud

environment12.

NO.26 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 whether 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 whether the strategy is developed by both cloud service providers and cloud service consumers within the acceptable limits of their risk appetite.
* Validate whether 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.

NO.27 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?
* Perform a risk analysis.
* Escalate to senior management.
* Review the procurement process.
* Review the business impact analysis (BIA).

NO.28 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 (CSA) and validated audit reports of the cloud service providers.
* validate an understanding of the organization’s current state and how the cloud audit plan fits into the existing audit approach.
* validate the organization’s performance effectiveness utilizing cloud service provider solutions.
* validate whether an organization has a cloud audit plan in place.
According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, the primary objective for an auditor to understand the organization’s context for a cloud audit is to validate an understanding of the organization’s current state and how the cloud audit plan fits into the existing audit approach1. The auditor should consider the organization’s business objectives, strategies, risks, and opportunities, as well as the regulatory and contractual requirements that apply to the organization’s use of cloud services. The auditor should also assess the organization’s cloud maturity level, governance structure, policies and procedures, roles and responsibilities, and existing controls related to cloud services. The auditor should then align the cloud audit plan with the organization’s context and ensure that it covers the relevant scope, objectives, criteria, and methodology.

The other options are not the primary objective for an auditor to understand the organization’s context for a cloud audit. Option A is a possible audit procedure, but not the main goal of understanding the organization’s context. Option C is a possible audit outcome, but not the main purpose of understanding the organization’s context. Option D is a possible audit finding, but not the main reason for understanding the organization’s context. Reference:

ISACA Cloud Auditing Knowledge Certificate Study Guide, page 12-13.

NO.29 Which of the following aspects of risk management involves identifying the potential reputational and financial harm when an incident occurs?
* Likelihood
* Mitigation
* Residual risk
* Impact analysis
Impact analysis is the aspect of risk management that involves identifying the potential reputational and financial harm when an

incident occurs. Impact analysis is the process of estimating the consequences or effects of a risk event on the business objectives, operations, processes, or functions. Impact analysis helps to measure and quantify the severity or magnitude of the risk event, as well as to prioritize and rank the risks based on their impact. Impact analysis also helps to determine the appropriate level of response and mitigation for each risk event, as well as to allocate the necessary resources and budget for risk management123.

Likelihood (A) is not the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Likelihood is the aspect of risk management that involves estimating the probability or frequency of a risk event occurring. Likelihood is the process of assessing and evaluating the factors or causes that may trigger or influence a risk event, such as threats, vulnerabilities, assumptions, uncertainties, etc. Likelihood helps to measure and quantify the chance or possibility of a risk event happening, as well as to prioritize and rank the risks based on their likelihood123.

Mitigation (B) is not the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Mitigation is the aspect of risk management that involves reducing or minimizing the likelihood or impact of a risk event. Mitigation is the process of implementing and applying controls or actions that can prevent, avoid, transfer, or accept a risk event, depending on the risk appetite and tolerance of the organization. Mitigation helps to improve and enhance the security and resilience of the organization against potential risks, as well as to optimize the cost and benefit of risk management123.

Residual risk © is not the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Residual risk is the aspect of risk management that involves measuring and monitoring the remaining or leftover risk after mitigation. Residual risk is the process of evaluating and reviewing the effectiveness and efficiency of the mitigation controls or actions, as well as identifying and addressing any gaps or issues that may arise. Residual risk helps to ensure that the actual level of risk is aligned with the desired level of risk, as well as to update and improve the risk management strategy and plan123. Reference := Risk Analysis: A Comprehensive Guide | SafetyCulture Risk Assessment and Analysis Methods: Qualitative and Quantitative – ISACA Risk Management Process – Risk Management | Risk Assessment | Risk …

NO.30 The PRIMARY purpose of Open Certification Framework (OCF) for the CSA STAR program is to:
* facilitate an effective relationship between the cloud service provider and cloud client.
* enable the cloud service provider to prioritize resources to meet its own requirements.
* provide global, accredited, and trusted certification of the cloud service provider.
* ensure understanding of true risk and perceived risk by the cloud service users

Explanation

The primary purpose of the Open Certification Framework (OCF) for the CSA STAR program is to provide global, accredited, and trusted certification of the cloud service provider. According to the CSA website1, the OCF is an industry initiative to allow global, trusted independent evaluation of cloud providers. It is a program for flexible, incremental and multi-layered cloud provider certification and/or attestation according to the Cloud Security Alliance’s industry leading security guidance and control framework. The OCF aims to address the gaps within the IT ecosystem that are inhibiting market adoption of secure and reliable cloud services. The OCF also integrates with popular third-party assessment and attestation statements developed within the public accounting community to avoid duplication of effort and cost. The OCF manages the foundation that runs and monitors the CSA STAR Certification program, which is an assurance framework that enables cloud service providers to embed cloud-specific security controls. The STAR Certification program has three levels of assurance, each based on a different type of audit or assessment: Level 1: Self-Assessment, Level 2:

Third-Party Audit, and Level 3: Continuous Auditing. The OCF also oversees the CSA STAR Registry, which is a publicly accessible repository that documents the security controls provided by various cloud computing offerings2. The OCF helps consumers to evaluate and compare their providers’ resilience, data protection, privacy capabilities, and service portability. It also helps providers to demonstrate their compliance with industry standards and best practices.

References:

Open Certification Framework Working Group | CSA

STAR | CSA

NO.31 What is the newer application development methodology and philosophy focused on automation of application development and deployment?
* Agile
* BusOps
* DevOps
* SecDevOps
* Scrum

NO.32 Which of the following is a direct benefit of mapping the Cloud Control Matrix (CCM) to other international standards and regulations?
* CCM mapping entitles cloud service providers to be listed as an approved supplier for tenders and government contracts.
* CCM mapping enables cloud service providers and customers alike to streamline their own compliance and security efforts.
* CCM mapping enables an uninterrupted data flow and, in particular, the export of personal data across different jurisdictions.
* CCM mapping entitles cloud service providers to be certified under the CSA STAR program.

NO.33 A dot release of the Cloud Controls Matrix (CCM) indicates:
* a revision of the CCM domain structure.
* a technical change (revision, addition, or deletion) of a number of controls that is smaller than 10% compared to the previous full release.
* the introduction of new control frameworks mapped to previously published CCM controls.
* technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release.

A dot release of the Cloud Controls Matrix (CCM) indicates a technical change (revision, addition, or deletion) of a number of controls that is smaller than 10% compared to the previous full release. A dot release is a minor update to the CCM that reflects the feedback from the cloud security community and the changes in the cloud technology landscape. A dot release does not change the domain structure or the overall scope of the CCM, but rather improves the clarity, accuracy, and relevance of the existing controls. A dot release is denoted by a decimal number after the major version number, such as CCM v4.1 or CCM v4.2. The current version of the CCM is v4.0, which was released in October 20211.

The other options are incorrect because:

* A. a revision of the CCM domain structure: A revision of the CCM domain structure is a major change that affects the organization and categorization of the controls into different domains. A revision of the CCM domain structure requires a full release, not a dot release, and is denoted by an integer number, such as CCM v3 or CCM v42.

* C. the introduction of new control frameworks mapped to previously published CCM controls: The introduction of new control frameworks mapped to previously published CCM controls is an additional feature that enhances the usability and applicability of the CCM. The introduction of new control frameworks mapped to previously published CCM controls does not require a dot release or a full release, but rather an update to the mapping table that shows the relationship between the CCM controls and other industry-accepted security standards, regulations, and frameworks3.

* D. technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release: A technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release is a significant change that affects the content and scope of the CCM. A technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release requires a full release, not a dot release, and is denoted by an integer number, such as CCM v3 or CCM v42.

References:

* Cloud Controls Matrix (CCM) – CSA

* The CSA Cloud Controls Matrix (CCM) V4: Raising the cloud security bar

* Cloud Security Alliance Releases New Cloud Controls Matrix Auditing Guidelines

NO.34 An organization is using the Cloud Controls Matrix (CCM) to extend its IT governance in the cloud. Which of the following is the BEST way for the organization to take advantage of the supplier relationship feature?
* Filter out only those controls directly influenced by contractual agreements.
* Leverage this feature to enable the adoption of the Shared Responsibility Model.
* Filter out only those controls having a direct impact on current terms of service (TOS) and service level agreement (SLA).
* Leverage this feature to enable a smarter selection of the next cloud provider.
Explanation

The best way for the organization to take advantage of the supplier relationship feature of the Cloud Controls Matrix (CCM) is to leverage this feature to enable a smarter selection of the next cloud provider. The supplier relationship feature is a column in the CCM spreadsheet that indicates whether a control is influenced by contractual agreements between the cloud service provider and the cloud customer. This feature can help the organization to identify and compare the security and compliance capabilities of different cloud providers, as well as to negotiate and customize the terms of service (TOS) and service level agreements (SLA) according to their needs and requirements123.

The other options are not the best ways to use the supplier relationship feature. Option A, filter out only those controls directly influenced by contractual agreements, is not a good way to use the feature because it would exclude other important controls that are not influenced by contractual agreements, but still relevant for cloud security and governance. Option B, leverage this feature to enable the adoption of the Shared Responsibility Model, is not a good way to use the feature because the Shared Responsibility Model is defined by another column in the CCM spreadsheet, which indicates whether a control is applicable to the cloud service provider or the cloud customer. Option C, filter out only those controls having a direct impact on current TOS and SLA, is not a good way to use the feature because it would exclude other controls that may have an indirect or potential impact on the TOS and SLA, or that may be subject to change or negotiation in the future. References

:=

What is CAIQ? | CSA – Cloud Security Alliance1

Understanding the Cloud Control Matrix | CloudBolt Software3

Cloud Controls Matrix (CCM) – CSA2

NO.35 Which of the following is an example of a corrective control?
* A central antivirus system installing the latest signature files before allowing a connection to the network
* All new employees having standard access rights until their manager approves privileged rights
* Unsuccessful access attempts being automatically logged for investigation
* Privileged access to critical information systems requiring a second factor of authentication using a soft token
A corrective control is a measure taken to correct or reduce the impact of an error, deviation, or unwanted activity1. Corrective control can be either manual or automated, depending on the type of control used. Corrective control can involve procedures, manuals, systems, patches, quarantines, terminations, reboots, or default dates1. A Business Continuity Plan (BCP) is an example of a corrective control.

Unsuccessful access attempts being automatically logged for investigation is an example of a corrective control because it is a response to a potential security incident that aims to identify and resolve the cause and prevent future occurrences2. Logging and investigating failed login attempts can help detect unauthorized or malicious attempts to access sensitive data or systems and take appropriate actions to mitigate the risk.

The other options are examples of preventive controls, which are designed to prevent problems from occurring in the first place3. Preventive controls can include:

A central antivirus system installing the latest signature files before allowing a connection to the network: This is a preventive control because it prevents malware infection by blocking potentially harmful connections and updating the antivirus software regularly4.

All new employees having standard access rights until their manager approves privileged rights: This is a preventive control because it prevents unauthorized access by enforcing the principle of least privilege and requiring approval for granting higher-level permissions5.

Privileged access to critical information systems requiring a second factor of authentication using a soft token: This is a preventive control because it prevents credential theft or compromise by adding an extra layer of security to verify the identity of the user.

Reference:

What is a corrective control? – Answers1, section on Corrective control Detective controls – SaaS Lens – docs.aws.amazon.com2, section on Unsuccessful login attempts Internal control: how do preventive and detective controls work?3, section on Preventive Controls What Are Security Controls? – F54, section on Preventive Controls The 3 Types of Internal Controls (With Examples) | Layer Blog5, section on Preventive Controls What are the 3 Types of Internal Controls? – RiskOptics – Reciprocity, section on Preventive Controls

NO.36 When applying the Top Threats Analysis methodology following an incident, what is the scope of the technical impact identification step?
* Determine the impact on confidentiality, integrity, and availability of the information system.
* Determine the impact on the physical and environmental security of the organization, excluding informational assets.
* Determine the impact on the controls that were selected by the organization to respond to identified risks.
* Determine the impact on the financial, operational, compliance, and reputation of the

Explanation

When applying the Top Threats Analysis methodology following an incident, the scope of the technical impact identification step is to determine the impact on confidentiality, integrity, and availability of the information system. The Top Threats Analysis methodology is a process developed by the Cloud Security Alliance (CSA) to help organizations identify, analyze, and mitigate the top threats to cloud computing, as defined in the CSA Top Threats reports. The methodology consists of six steps1:

Scope definition: Define the scope of the analysis, such as the cloud service model, deployment model, and business context.

Threat identification: Identify the relevant threats from the CSA Top Threats reports that may affect the scope of the analysis.

Technical impact identification: Determine the impact on confidentiality, integrity, and availability of the information system caused by each threat. Confidentiality refers to the protection of data from unauthorized access or disclosure. Integrity refers to the protection of data from unauthorized modification or deletion. Availability refers to the protection of data and services from disruption or denial.

Business impact identification: Determine the impact on the business objectives and operations caused by each threat, such as financial loss, reputational damage, legal liability, or regulatory compliance.

Risk assessment: Assess the likelihood and severity of each threat based on the technical and business impacts, and prioritize the threats according to their risk level.

Risk treatment: Select and implement appropriate risk treatment options for each threat, such as avoidance, mitigation, transfer, or acceptance.

The technical impact identification step is important because it helps to measure the extent of damage or harm that each threat can cause to the information system and its components. This step also helps to align the technical impacts with the business impacts and to support the risk assessment and treatment steps.

References := CCAK Study Guide, Chapter 4: A Threat Analysis Methodology for Cloud Using CCM, page

81

NO.37 Which of the following statements are NOT requirements of governance and enterprise risk management in a cloud environment?
* Inspect and account for risksinherited from other members of the cloud supply chain and take active measures to mitigate and contain risks through operational resiliency.
* Respect the interdependency of the risks inherent in the cloud supply chain and communicate the corporate riskposture and readiness to consumers and dependent parties.
* Negotiate long-term contracts with companies who use well-vetted software application to avoid the transient nature of the cloud environment.
* Provide transparency to stakeholders and shareholders demonstrating fiscal solvency and organizational transparency.
* Both B and C.

NO.38 When applying the Top Threats Analysis methodology following an incident, what is the scope of the technical impact identification step?
* Determine the impact on the controls that were selected by the organization to respond to identified risks.
* Determine the impact on confidentiality, integrity, and availability of the information system.
* Determine the impact on the physical and environmental security of the organization, excluding informational assets.
* Determine the impact on the financial, operational, compliance, and reputation of the organization.

Explanation

When applying the Top Threats Analysis methodology following an incident, the scope of the technical impact identification step is to determine the impact on confidentiality, integrity, and availability of the information system. The Top Threats Analysis methodology is a framework developed by the Cloud Security Alliance (CSA) to help organizations identify, analyze, and mitigate the most critical threats to cloud computing. The methodology consists of six steps: threat identification, threat analysis, technical impact identification, business impact analysis, risk assessment, and risk treatment12.

The technical impact identification step is the third step of the methodology, and it aims to assess how the incident affected the security properties of the information system, namely confidentiality, integrity, and availability. Confidentiality refers to the protection of data from unauthorized access or disclosure. Integrity refers to the protection of data from unauthorized modification or deletion. Availability refers to the protection of data and services from disruption or denial. The technical impact identification step can help organizations to understand the severity and extent of the incident and its consequences on the information system12.

The other options are not within the scope of the technical impact identification step. Option A, determine the impact on the controls that were selected by the organization to respond to identified risks, is not within the scope because it is part of the risk treatment

step, which is the sixth and final step of the methodology. Option C, determine the impact on the physical and environmental security of the organization, excluding informational assets, is not within the scope because it is not related to the information system or its security properties. Option D, determine the impact on the financial, operational, compliance, and reputation of the organization, is not within the scope because it is part of the business impact analysis step, which is the fourth step of the methodology. References := Top Threats Analysis Methodology – CSA1 Top Threats Analysis Methodology – Cloud Security Alliance