Free Questions for CCAK by dumpssheet

Shared by Petersen on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

If a customer management interface is compromised over the public Internet, it can lead to:

Options:

A- incomplete wiping of the data.

B- computing and data compromise for customers.

C- ease of acquisition of cloud services.

D- access to the RAM of neighboring cloud computers.

Answer:

B

Explanation:

Customer management interfaces are the web portals or applications that allow customers to access and manage their cloud services, such as provisioning, monitoring, billing, etc. These interfaces are exposed to the public Internet and may be vulnerable to attacks such as phishing, malware, denial-of-service, or credential theft. If an attacker compromises a customer management interface, they can potentially access and manipulate the customer's cloud resources, data, and configurations, leading to computing and data compromise for customers. This can result in data breaches, service disruptions, unauthorized transactions, or other malicious activities.

Cloud Computing - Security Benefits and Risks | PPT - SlideShare1, slide 10

Cloud Security Risks: The Top 8 According To ENISA - CloudTweaks2, section on Management Interface Compromise

Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, section 2.3.2.1 : https://www.isaca.org/-/media/info/ccak/ccak-study-guide.pdf

Question 2

Question Type: MultipleChoice

Why should the results of third-party audits and certification be relied on when analyzing and assessing the cybersecurity risks in the cloud?

Options:

A- To establish an audit mindset within the organization

B- To contrast the risk generated by the loss of control

C- To reinforce the role of the internal audit function

D- To establish an accountability culture within the organization

Answer:

B

Explanation:

One possible reason why the results of third-party audits and certification should be relied on when analyzing and assessing the cybersecurity risks in the cloud is to contrast the risk generated by the loss of control.When an organization moves its data and processes to the cloud, it inevitably loses some degree of control over its security and compliance posture, as it depends on the cloud service provider (CSP) to implement and maintain adequate security measures and controls1This loss of control can increase the organization's exposure to various cybersecurity risks, such as data breaches, unauthorized access, denial of service, malware infection, etc2

To mitigate these risks, the organization needs to have a clear understanding of the security and compliance level of the CSP, as well as the shared responsibility model that defines the roles and responsibilities of both parties3Third-party audits and certification can provide some level of assurance that the CSP meets certain standards and requirements related to security and compliance, such as ISO/IEC 27001, CSA STAR, SOC 2, etc. These audits and certification can also help the organization compare and contrast the security posture of different CSPs in the market, as well as identify any gaps or weaknesses that need to be addressed or compensated.

Therefore, relying on the results of third-party audits and certification can help the organization contrast the risk generated by the loss of control in the cloud, and make informed decisions about selecting and managing its cloud services.

Question 3

Question Type: **MultipleChoice**

A certification target helps in the formation of a continuous certification framework by incorporating:

Options:

A- the service level objective (SLO) and service qualitative objective (SQO).

B- the scope description and security attributes to be tested.

C- the frequency of evaluating security attributes.

D- CSA STAR level 2 attestation.

Answer:

B

Explanation:

According to the blog article "Continuous Auditing and Continuous Certification" by the Cloud Security Alliance, a certification target helps in the formation of a continuous certification framework by incorporating the scope description and security attributes to be tested1A certification target is a set of security objectives that a cloud service provider (CSP) defines and commits to fulfill as part of the continuous certification process1Each security objective is associated with a policy that specifies the assessment frequency, such as every four hours, every day, or every week1A certification target also includes a set of tools that are capable of verifying that the security objectives are met, such as automated scripts, APIs, or third-party services1

The other options are not correct because:

Option A is not correct because the service level objective (SLO) and service qualitative objective (SQO) are not part of the certification target, but rather part of the service level agreement (SLA) between the CSP and the cloud customer. An SLO is a measurable characteristic of the cloud service, such as availability, performance, or reliability.An SQO is a qualitative characteristic of the cloud service, such as security, privacy, or compliance2The SLA defines the expected level of service and the consequences of not meeting it. The SLA may be used as an input for defining the certification target, but it is not equivalent or synonymous with it.

Option C is not correct because the frequency of evaluating security attributes is not the only component of the certification target, but rather one aspect of it. The frequency of evaluating security attributes is determined by the policy that is associated with each security objective in the certification target.The policy defines how often the security objective should be verified by the tools, such as every four hours, every day, or every week1However, the frequency alone does not define the certification target, as it also depends on the scope description and the security attributes to be tested.

Option D is not correct because CSA STAR level 2 attestation is not a component of the certification target, but rather a prerequisite for it.CSA STAR level 2 attestation is a third-party independent assessment of the CSP's security posture based on ISO/IEC 27001 and CSA Cloud Controls Matrix (CCM)3CSA STAR level 2 attestation provides a baseline assurance level for the CSP before they can define and implement their certification target for continuous certification.CSA STAR level 2 attestation is also required for CSA STAR level 3 certification, which is based on continuous auditing and continuous certification3

Question 4

Question Type: MultipleChoice

An auditor identifies that a cloud service provider received multiple customer inquiries and requests for proposal (RFPs) during the last month.

Which of the following should be the BEST recommendation to reduce the provider's burden?

Options:

A- The provider can schedule a call with each customer.

B- The provider can share all security reports with customers to streamline the process.

C- The provider can answer each customer individually.

D- The provider can direct all customer inquiries to the information in the CSA STAR registry

Answer:

D

Explanation:

The CSA STAR registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings1The registry is designed for users of cloud services to assess their cloud providers' security and compliance posture, including the regulations, standards, and frameworks they adhere to1The registry also promotes industry transparency and reduces complexity and costs for both providers and customers2

The provider can direct all customer inquiries to the information in the CSA STAR registry, as this would be the best recommendation to reduce the provider's burden.By publishing to the registry, the provider can show current and potential customers their security and compliance posture, without having to fill out multiple customer questionnaires or requests for proposal (RFPs)2The provider can also leverage the different levels of assurance available in the registry, such as self-assessment, third-party audit, or certification, to demonstrate their security maturity and trustworthiness1The provider can also benefit from the CSA Trusted Cloud Providers program, which recognizes providers that have fulfilled additional training and volunteer requirements with CSA, demonstrating their commitment to cloud security competency and industry best practices3

The other options are not correct because:

Option A is not correct because the provider can schedule a call with each customer is not a good recommendation to reduce the provider's burden. Scheduling a call with each customer would be time-consuming, inefficient, and impractical, especially if the provider receives multiple inquiries and RFPs every month. Scheduling a call would also not guarantee that the customer would be satisfied with the provider's security and compliance posture, as they may still request additional information or evidence. Scheduling a call would also not help the provider differentiate themselves from other providers in the market, as they may not be able to showcase their security maturity and trustworthiness effectively.

Option B is not correct because the provider can share all security reports with customers to streamline the process is not a good recommendation to reduce the provider's burden. Sharing all security reports with customers may not be feasible, as some reports may contain sensitive or confidential information that should not be disclosed to external parties. Sharing all security reports may also not be desirable, as some reports may be outdated, incomplete, or inconsistent, which could undermine the provider's credibility and reputation. Sharing all security reports may also not be effective, as some customers may not have the expertise or resources to review and understand them properly.

Option C is not correct because the provider can answer each customer individually is not a good recommendation to reduce the provider's burden. Answering each customer individually would be tedious, repetitive, and costly, as the provider would have to provide similar or identical information to different customers over and over again. Answering each customer individually would also not ensure that the provider's security and compliance posture is consistent and accurate, as they may make mistakes or omissions in their responses. Answering each customer individually would also not help the provider stand out from other providers in the market, as they may not be able to highlight their security achievements and certifications.

Question 5

Question Type: MultipleChoice

To ensure integration of security testing is implemented on large code sets in environments where time to completion is critical, what form of validation should an auditor expect?

Options:

A- Parallel testing

B- Full application stack unit testing

C- Functional verification

D- Regression testing

Answer:

D

Explanation:

Regression testing is a type of software testing that confirms that a recent program or code change has not adversely affected existing features1It involves re-running functional and non-functional tests to ensure that previously developed and tested software still performs as expected after a change2Regression testing is suitable for large code sets in environments where time to completion is critical, as it can help detect and prevent defects, improve quality, and enable faster delivery of secure software.Regression testing can be automated to reduce manual errors, speed up feedback loops, and increase efficiency and reliability3

The other options are not correct because:

Option A is not correct because parallel testing is a type of software testing that involves testing multiple applications or subsystems concurrently to reduce the test time4Parallel testing does not necessarily ensure the integration of security testing, as it depends on the quality and coverage of the test cases and scenarios used for each application or subsystem.Parallel testing may also introduce challenges such as synchronization, coordination, and communication among the testers and developers5

Option B is not correct because full application stack unit testing is a type of software testing that involves testing individual units or components of an application in isolation to verify their functionality, logic, interfaces, and performance6Full application stack unit testing does not ensure the integration of security testing, as it does not consider the interactions and dependencies among the units or components, or the behavior of the application as a whole.Unit testing is typically performed by developers at an early stage of the software development life cycle, and may not cover all the security aspects or requirements of the application7

Option C is not correct because functional verification is a type of software testing that involves verifying that the software meets the specified requirements and satisfies the user needs. Functional verification does not ensure the integration of security testing, as it does not focus on how the software is designed or configured, or how it handles malicious or unexpected inputs. Functional verification is typically performed by quality assurance teams at a later stage of the software development life cycle, and may not detect all the security vulnerabilities or risks of the software.

Question 6

Question Type: MultipleChoice

The MOST important goal of regression testing is to ensure:

Options:

A- the expected outputs are provided by the new features.

B- the system can handle a high number of users.

C- the system can be restored after a technical issue.

D- new releases do not impact previous stable features.

Answer:

D

Explanation:

According to the definition of regression testing, it is a type of software testing that confirms that a recent program or code change has not adversely affected existing features1It involves re-running functional and non-functional tests to ensure that previously developed and tested software still performs as expected after a change2If the software does not perform as expected, it is called a regression. Therefore, the most important goal of regression testing is to ensure new releases do not impact previous stable features.

The other options are not correct because:

Option A is not correct because the expected outputs are provided by the new features is not the goal of regression testing, but rather the goal of functional testing or acceptance testing. These types of testing aim to verify that the software meets the specified requirements and satisfies the user needs.Regression testing, on the other hand, focuses on checking that the existing features are not broken by the new features3

Option B is not correct because the system can handle a high number of users is not the goal of regression testing, but rather the goal of performance testing or load testing. These types of testing aim to evaluate the behavior and responsiveness of the software under various workloads and conditions.Regression testing, on the other hand, focuses on checking that the software functionality and quality are not degraded by code changes4

Option C is not correct because the system can be restored after a technical issue is not the goal of regression testing, but rather the goal of recovery testing or disaster recovery testing. These types of testing aim to assess the ability of the software to recover from failures or disasters and resume normal operations.Regression testing, on the other hand, focuses on checking that the software does not introduce new failures or defects due to code changes5

Question 7

Question Type: MultipleChoice

DevSecOps aims to integrate security tools and processes directly into the software development life cycle and should be done:

Options:

A- at the end of the development cycle.

B- after go-live.

C- in all development steps.

D- at the beginning of the development cycle.

Answer:

A

Explanation:

According to the CCAK Study Guide, the business continuity management and operational resilience strategy of the cloud customer should be formulated jointly with the cloud service provider, as they share the responsibility for ensuring the availability and recoverability of the cloud services. The strategy should cover 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. These activities include prevention, mitigation, response, recovery, restoration, and improvement.The strategy should also define the roles and responsibilities of both parties, the communication channels and escalation procedures, the testing and exercising plans, and the review and update mechanisms1

The other options are not correct because:

Option B is not correct because the strategy should not only be developed within the acceptable limits of the risk appetite, but also aligned with the business objectives and stakeholder expectations of both parties.The risk appetite is only one of the factors that influence the strategy formulation1

Option C is not correct because the strategy should not only cover the activities required to continue and recover prioritized activities within identified time frames and agreed capacity, but also consider the activities for before and after a disruption, such as prevention, mitigation, improvement, etc.The strategy should also include other elements such as roles and responsibilities, communication channels, testing plans, etc1

20%
DISCOUNT