Isaca

Exam Questions CCAK

Certificate of Cloud Auditing Knowledge

NEW QUESTION 1
The Cloud Octagon Model was developed to support organizations':

A. risk treatment methodology.
B. incident detection methodology.
C. incident response methodology.
D. risk assessment methodology.

Answer: D

Explanation:
The Cloud Octagon Model was developed to support organizations?? risk assessment methodology. Risk assessment is the process of identifying, analyzing, and evaluating the risks associated with a cloud computing environment. The Cloud Octagon Model provides a logical approach to holistically deal with security aspects involved in moving to the cloud by introducing eight dimensions that need to be considered: procurement, IT governance, architecture, development and engineering, service
providers, risk processes, data classification, and country. The model aims to reduce risks, improve effectiveness, manageability, and security of cloud solutions12.
References:
? Cloud Octagon Model | CSA
? Cloud Security Alliance Releases Cloud Octagon Model

NEW QUESTION 2
Organizations maintain mappings between the different control frameworks they adopt to:

A. help identify controls with common assessment status.
B. avoid duplication of work when assessing compliance,
C. help identify controls with different assessment status.
D. start a compliance assessment using the latest assessment.

Answer: B

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 3
Regarding suppliers of a cloud service provider, it is MOST important for the auditor to be aware that the:

A. client organization does not need to worry about the provider's suppliers, as this is the provider's responsibility.
B. suppliers are accountable for the provider's service that they are providing.
C. client organization and provider are both responsible for the provider's suppliers.
D. client organization has a clear understanding of the provider's suppliers.

Answer: D

Explanation:
It is most important for the auditor to be aware that the client organization has a clear understanding of the provider??s suppliers. The provider??s suppliers are the third- party entities that provide services or products to the provider, such as infrastructure, software, hardware, or support. The provider??s suppliers may have a significant impact on the quality, security, reliability, and performance of the cloud services that the provider delivers to the client organization. Therefore, the auditor should ensure that the client organization knows who the provider??s suppliers are, what services or products they provide, what risks they pose, and what contractual or regulatory obligations they have123. The other options are not correct. Option A, the client organization does not need to worry about the provider??s suppliers, as this is the provider??s responsibility, is incorrect because
the client organization cannot rely solely on the provider to manage its suppliers. The client organization has to perform due diligence and oversight on the provider??s suppliers, as they may affect the client organization??s own security, compliance, and business objectives12. Option B, the suppliers are accountable for the provider??s service that they are providing, is incorrect because the suppliers are not directly accountable to the client organization, but
to the provider. The provider is ultimately accountable to the client organization for its
service delivery and performance12. Option C, the client organization and provider are both responsible for the provider??s suppliers, is incorrect because the responsibility for the provider??s suppliers depends on the shared responsibility model, which defines how the security and compliance tasks and obligations are divided between the provider and the client organization. The shared responsibility model may vary depending on the type and level of cloud service that the provider offers12. References :=
? Cloud Computing: Auditing Challenges - ISACA1
? Cloud Computing: Audit Considerations - ISACA2
? Top 16 Cloud Computing Companies & Service Providers 2023 - Datamation

NEW QUESTION 4
Which of the following BEST describes the difference between a Type 1 and a Type 2 SOC report?

A. A Type 2 SOC report validates the operating effectiveness of controls, whereas a Type 1 SOC report validates the suitability of the design of the controls.
B. A Type 1 SOC report provides an attestation, whereas a Type 2 SOC report offers a certification.
C. A Type 2 SOC report validates the suitability of the control design, whereas a Type 1 SOC report validates the operating effectiveness of controls.
D. There is no difference between a Type 2 and a Type 1 SOC report.

Answer: A

Explanation:

A Type 1 SOC report assesses whether controls are appropriately designed at a specific point in time, while a Type 2 SOC report tests the operating effectiveness of these controls over a period. For cloud auditing, Type 2 is often preferred for its comprehensive approach to both design and effectiveness over time. The CCAK curriculum emphasizes understanding these reports as critical tools in auditing cloud service providers (referenced in the CCAK content on Assurance and Transparency and the CSA STAR framework).
=========================

NEW QUESTION 5
An organization employing the Cloud Controls Matrix (CCM) to perform a compliance assessment leverages the Scope Applicability direct mapping to:

A. obtain the ISO/IEC 27001 certification from an accredited certification body (CB) following the ISO/IEC 17021-1 standard.
B. determine whether the organization can be considered fully compliant with the mapped standards because of the implementation of every CCM Control Specification.
C. understand which controls encompassed by the CCM may already be partially or fully implemented because of the compliance with other standards.

Answer: C

Explanation:
An organization employing the Cloud Controls Matrix (CCM) to perform a compliance assessment leverages the Scope Applicability direct mapping to understand which controls encompassed by the CCM may already be partially or fully implemented because of the compliance with other standards. The Scope Applicability direct mapping is a worksheet within the CCM that maps the CCM control specifications to several standards within the ISO/IEC 27000 series, such as ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, and ISO/IEC 27018. The mapping helps the organization to identify the commonalities and differences between the CCM and the ISO/IEC standards, and to determine the level of compliance with each standard based on the implementation of the CCM controls. The mapping also helps the organization to avoid duplication of work and to streamline the
compliance assessment process.12 References := What you need to know: Transitioning CSA STAR for Cloud Controls Matrix ??1; Cloud Controls Matrix (CCM) - CSA3

NEW QUESTION 6
A large healthcare provider within the United States is seeking a cloud service provider offering Software as a Service (SaaS) for core business systems. The selected provider MUST comply with which of the following regulations?

A. GDPR
B. HIPAA
C. GLBA
D. FISMA

Answer: B

NEW QUESTION 7
Which of the following is the MOST relevant question in the cloud compliance program design phase?

A. Who owns the cloud services strategy?
B. Who owns the cloud strategy?
C. Who owns the cloud governance strategy?
D. Who owns the cloud portfolio strategy?

Answer: B

Explanation:
The most relevant question in the cloud compliance program design phase is who owns the cloud governance strategy. Cloud governance is a method of information and technology (I&T) governance focused on accountability, defining decision rights and balancing benefit, risk and resources in an environment that embraces cloud
computing. Cloud governance creates business-driven policies and principles that establish the appropriate degree of investments and control around the life cycle process for cloud computing services1. Therefore, it is essential to identify who owns the cloud governance strategy in the organization, as this will determine the roles and responsibilities, decision- making authority, reporting structure, and escalation process for cloud compliance issues. The cloud governance owner should be a senior executive who has the vision, influence, and resources to drive the cloud compliance program and align it with the business objectives2.
References:
? Building Cloud Governance From the Basics - ISACA
? [Cloud Governance | Microsoft Azure]

NEW QUESTION 8
Which of the following is the BEST recommendation to offer an organization's HR department planning to adopt a new public Software as a Service (SaaS) application to ease the recruiting process?

A. Implement a cloud access security broker (CASB).
B. Do not allow data to be in clear text.
C. Ensure HIPAA compliance.
D. Consult the legal department.

Answer: A

NEW QUESTION 9
Which of the following is an example of reputational business impact?

A. While the breach was reported in a timely manner to the CEO, the CFO and CISO blamed each other in public, resulting in a loss of public confidence that led the board to replace all three.
B. The cloud provider fails to report a breach of customer personal data from an unsecured server, resulting in GDPR fines of 10 million euros.
C. A distributed denial of service (DDoS) attack renders the customer??s cloud inaccessiblefor 24 hours, resulting in millions in lost sales.
D. A hacker using a stolen administrator identity brings down the Software as a Service (SaaS) sales and marketing systems, resulting in the inability to process

customer orders or manage customer relationships.

Answer: A

Explanation:
Reputational business impact refers to the effect on a company??s reputation and public perception following an incident or action. Option A is an example of reputational impact because the public dispute among high-level executives after a breach was reported reflects poorly on the company??s governance and crisis management capabilities. This public display of discord can erode stakeholder trust and confidence, potentially leading to a decline in the company??s market value, customer base, and ability to attract and retain talent.
References = The answer is derived from the understanding of reputational risk and its consequences on businesses, as discussed in various cloud auditing and security resources. Reputational impact is a key consideration in the governance of cloud operations, which is a topic covered in the CCAK curriculum1234.

NEW QUESTION 10
The MOST important goal of regression testing is to ensure:

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 features1 It involves re-running functional and non-functional tests to ensure that previously developed and tested software still performs as expected after a change2 If 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
References: 1: Wikipedia. Regression testing - Wikipedia. [Online]. Available: 3. [Accessed: 14-Apr-2023]. 2: Katalon. What is Regression Testing? Definition, Tools, Examples -
Katalon. [Online]. Available: 4. [Accessed: 14-Apr-2023]. 3: Guru99. What is Functional Testing? Types & Examples - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023]. 4: Guru99. What is Performance Testing? Types & Examples - Guru99. [Online]. Available:
. [Accessed: 14-Apr-2023]. 5: Guru99. What is Recovery Testing? with Example - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023].

NEW QUESTION 10
Which of the following is an example of financial business impact?

A. A distributed denial of service (DDoS) attack renders the customer's cloud inaccessible for 24 hours, resulting in millions in lost sales.
B. A hacker using a stolen administrator identity brings down the Software of a Service (SaaS) sales and marketing systems, resulting in the inability to process customer orders or manage customer relationships.
C. While the breach was reported in a timely manner to the CEO, the CFO and CISO blamed each other in public consulting in a loss of public confidence that led the board to replace all three.

Answer: A

Explanation:
An example of financial business impact is a distributed denial of service (DDoS) attack that renders the customer??s cloud inaccessible for 24 hours, resulting in millions in lost sales. Financial business impact refers to the monetary losses or gains that an organization may experience as a result of a cloud security incident. Financial business impact can be measured by factors such as revenue, profit, cost, cash flow, market share, and stock price .
Option A is an example of financial business impact because it shows how a DDoS attack, which is a type of cyberattack that overwhelms a system or network with malicious traffic and prevents legitimate users from accessing it, can cause direct and significant financial losses for the customer??s organization due to the interruption of its cloud services and the inability to generate sales. Option A also implies that the customer??s organization depends on the availability of its cloud services for its core business operations.
The other options are not examples of financial business impact. Option B is an example of operational business impact, which refers to the disruption or degradation of the organization??s processes, functions, or activities as a result of a cloud security incident. Operational business impact can be measured by factors such as productivity, efficiency, quality, performance, and customer satisfaction . Option B shows how a hacker using a stolen administrator identity, which is a type of identity theft or impersonation attack that exploits the credentials or privileges of a legitimate user to access or manipulate a system or network, can cause operational business impact for the customer??s organization by bringing down its SaaS sales and marketing systems, which are essential for its business functions.
Option C is an example of reputational business impact, which refers to the damage or enhancement of the organization??s image, brand, or reputation as a result of a cloud security incident. Reputational business impact can be measured by factors such as trust, loyalty, satisfaction, awareness, and perception of the organization??s stakeholders, such as customers, partners, investors, regulators, and media . Option C shows how a breach reported in a timely manner to the CEO, which is a good practice for ensuring transparency and accountability in the event of a cloud security incident, can still cause reputational business impact for the customer??s organization due to the public blame game between the CFO and CISO, which reflects poorly on the organization??s leadership and culture and leads to the board replacing all three. References :=
? Business Impact Analysis - Ready.gov
? Business Impact Analysis - Cloud Security Alliance
? What Is A Distributed Denial-of-Service (DDoS) Attack? | Cloudflare
? What is Identity Theft? - Cloud Security Alliance

? Incident Response - Cloud Security Alliance

NEW QUESTION 15
Which of the following metrics are frequently immature?

A. Metrics around specific Software as a Service (SaaS) application services
B. Metrics around Infrastructure as a Service (laaS) computing environments
C. Metrics around Infrastructure as a Service (laaS) storage and network environments
D. Metrics around Platform as a Service (PaaS) development environments

Answer: D

Explanation:
Metrics around Platform as a Service (PaaS) development environments are frequently immature, as PaaS is a relatively new and evolving cloud service model that offers various tools and platforms for developing, testing, deploying, and managing cloud applications. PaaS metrics are often not well-defined, standardized, or consistent across different providers and platforms, and may not capture the full value and performance of PaaS services. PaaS metrics may also be difficult to measure, monitor, and compare, as they depend on various factors, such as the type, complexity, and quality of the
applications, the level of customization and integration, the usage patterns and demand, and the security and compliance requirements. Therefore, PaaS metrics may not provide sufficient insight or assurance to cloud customers and auditors on the effectiveness, efficiency, reliability, and security of PaaS services12.
References:
? Cloud Computing Service Metrics Description - NIST
? Cloud KPIs You Need to Measure Success - VMware Blogs

NEW QUESTION 20
The MOST critical concept for managing the building and testing of code in DevOps is:

A. continuous build.
B. continuous delivery.
C. continuous integration.
D. continuous deployment.

Answer: C

Explanation:
Continuous integration (CI) is the most critical concept for managing the building and testing of code in DevOps. CI is the practice of merging all developers?? working copies of code to a shared mainline several times a day. This enables early detection and resolution of bugs, conflicts, and errors, as well as faster and more frequent feedback loops. CI also facilitates the automation of building, testing, and deploying code, which improves the quality, reliability, and security of the software delivery process. CI is a prerequisite for continuous delivery (CD) and continuous deployment (CD), which are the next stages of DevOps maturity that aim to deliver software to customers faster and more frequently. References:
? ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p.114-115
? Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM) v4.0, 2021, DCS-01: Datacenter Security - Build and Test
? What is Continuous Integration?
? Continuous Integration vs Continuous Delivery vs Continuous Deployment

NEW QUESTION 25
Which of the following is the reason for designing the Consensus Assessments Initiative Questionnaire (CAIQ)?

A. Cloud service providers need the CAIQ to improve quality of customer service.
B. Cloud service providers can document their security and compliance controls.
C. Cloud service providers can document roles and responsibilities for cloud security.
D. Cloud users can use CAIQ to sign statement of work (SOW) with cloud access security

Answer: B

Explanation:
The reason for designing the Consensus Assessments Initiative Questionnaire (CAIQ) is to enable cloud service providers to document their security and compliance controls in a standardized and transparent way. The CAIQ is a set of yes/no questions that correspond to the controls of the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM), which is a framework of best practices for cloud security. The CAIQ helps cloud service providers to demonstrate their adherence to the CCM and to provide evidence of their security posture to potential customers, auditors, and regulators. The CAIQ also helps cloud customers and auditors to assess the security capabilities of cloud service providers and to compare different providers based on their responses. The CAIQ is part of the CSA STAR program, which is a cloud security assurance program that offers various levels of certification and attestation for cloud service providers.12 References := What is CAIQ? | CSA - Cloud Security Alliance3; Consensus Assessment Initiative Questionnaire (CAIQ) v3.1 [No | CSA4

NEW QUESTION 30
Which of the following processes should be performed FIRST to properly implement the NIST SP 800-53 r4 control framework in an organization?

A. A selection of the security objectives the organization wants to improve
B. A security categorization of the information systems
C. A comprehensive business impact analysis (BIA)
D. A comprehensive tailoring of the controls of the framework

Answer: B

Explanation:
A security categorization of the information systems should be performed first to properly implement the NIST SP 800-53 r4 control framework in an organization. Security categorization is the process of determining the potential impact on organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from a loss of confidentiality, integrity, or availability of an information system and the information processed, stored, or transmitted by that system. Security categorization is based on the application of FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, which defines three levels of impact: low, moderate, and high. Security categorization is the first step in the Risk Management Framework (RMF)

described in NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Security categorization helps to identify the security requirements for the information system and to select an initial set of baseline security controls from NIST SP 800-53 r4, Security and Privacy Controls for Federal Information Systems and Organizations. The baseline security controls can then be tailored and supplemented as needed to address specific organizational needs, risk factors, and compliance obligations12.
References:
? SP 800-53 Rev. 4, Security & Privacy Controls for Federal Info Sys ??
? SP 800-37 Rev. 2, Risk Management Framework for Information ??

NEW QUESTION 32
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?

A. Contractual documents of the cloud service provider
B. Heat maps
C. Data security process flow
D. Turtle diagram

Answer: B

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 37
Which of the following is an example of availability technical impact?

A. A distributed denial of service (DDoS) attack renders the customer's cloud inaccessible for 24 hours.
B. The cloud provider reports a breach of customer personal data from an unsecured server.
C. An administrator inadvertently clicked on phish bait, exposing the company to a ransomware attack.
D. A hacker using a stolen administrator identity alters the discount percentage in the product database

Answer: A

Explanation:
An example of availability technical impact is a distributed denial of service (DDoS) attack that renders the customer??s cloud inaccessible for 24 hours. Availability technical impact refers to the effect of a cloud security incident on the protection of data and services from disruption or denial. Availability is one of the three security properties of an information system, along with confidentiality and integrity.
Option A is an example of availability technical impact because it shows how a DDoS attack, which is a type of cyberattack that overwhelms a system or network with malicious traffic and prevents legitimate users from accessing it, can cause a severe and prolonged disruption of the customer??s cloud services. Option A also implies that the customer??s organization depends on the availability of its cloud services for its core business operations.
The other options are not examples of availability technical impact. Option B is an example of confidentiality technical impact, which refers to the effect of a cloud security incident on the protection of data from unauthorized access or disclosure. Option B shows how a breach of customer personal data from an unsecured server, which is a type of data leakage or exposure attack that exploits the lack of proper security controls on a system or network, can cause a violation of the privacy and security of the customer??s data. Option C is an example of integrity technical impact, which refers to the effect of a cloud security incident on the protection of data from unauthorized modification or deletion. Option C shows how an administrator inadvertently clicking on phish bait, which is a type of social engineering or phishing attack that tricks a user into clicking on a malicious link or attachment, can expose the company to a ransomware attack, which is a type of malware or encryption attack that locks or encrypts the data and demands a ransom for its release. Option D is also an example of integrity technical impact, as it shows how a hacker using a stolen administrator identity, which is a type of identity theft or impersonation attack that exploits the credentials or privileges of a legitimate user to access or manipulate a system or network, can alter the discount percentage in the product database, which is a type of data tampering or corruption attack that affects the accuracy and reliability of the data. References :=
? OWASP Risk Rating Methodology | OWASP Foundation1
? OEE Factors: Availability, Performance, and Quality | OEE2
? The Effects of Technological Developments on Work and Their ??

NEW QUESTION 39
What is the MOST effective way to ensure a vendor is compliant with the agreed-upon cloud service?

A. Examine the cloud provider's certifications and ensure the scope is appropriate.
B. Document the requirements and responsibilities within the customer contract
C. Interview the cloud security team and ensure compliance.
D. Pen test the cloud service provider to ensure compliance.

Answer: A

Explanation:
The most effective way to ensure a vendor is compliant with the agreed-upon cloud service is to examine the cloud provider??s certifications and ensure the scope is appropriate. Certifications are independent attestations of the cloud provider??s compliance with various standards, regulations, and best practices related to cloud security, privacy, and governance1. They provide assurance to customers that the cloud provider has implemented adequate controls and processes to meet their contractual obligations and expectations2. However, not all certifications are equally relevant or comprehensive, so customers need to verify that the certifications cover the specific cloud service, region, and data type that they are using3. Customers should also review the certification reports or audit evidence to understand the scope, methodology, and results of the assessment4.
The other options are not as effective as examining the cloud provider??s certifications. Documenting the requirements and responsibilities within the customer contract is an important step to establish the terms and conditions of the cloud service agreement, but it does not guarantee that the vendor will comply with them5. Customers need to monitor and verify the vendor??s performance and compliance on an ongoing basis. Interviewing the cloud security team may provide some insights into the vendor??s compliance practices, but it may not be sufficient or reliable without independent verification or documentation. Pen testing the cloud service provider may reveal some vulnerabilities or weaknesses in the vendor??s security posture, but it may not cover all aspects of compliance or be authorized by the vendor. Pen testing should be done with caution and consent, as it may cause disruption or damage to the cloud service or violate the terms of service.
References:
? Cloud Compliance: What You Need To Know - Linford & Company LLP1, section on Cloud Compliance
? Cloud Services Due Diligence Checklist | Trust Center2, section on Why Microsoft created the Cloud Services Due Diligence Checklist
? The top cloud providers for government | ZDNET3, section on What is FedRAMP?
? Cloud Computing Security Considerations | Cyber.gov.au4, section on Certification
? Cloud Audits and Compliance: What You Need To Know - Linford & Company LLP5, section on Cloud Compliance Management
? Cloud Services Due Diligence Checklist | Trust Center, section on How to use the checklist
? Cloud Computing Security Considerations | Cyber.gov.au, section on Security governance
? The top cloud providers for government | ZDNET, section on Penetration testing
? Penetration Testing in AWS - Amazon Web Services (AWS), section on Introduction

NEW QUESTION 41
Regarding suppliers of a cloud service provider, it is MOST important for the auditor to be aware that the:

A. client organization has a clear understanding of the provider s suppliers.
B. suppliers are accountable for the provider's service that they are providing.
C. client organization does not need to worry about the provider's suppliers, as this is the provider's responsibility.
D. client organization and provider are both responsible for the provider's suppliers.

Answer: A

Explanation:
Regarding suppliers of a cloud service provider, it is most important for the auditor to be aware that the client organization has a clear understanding of the provider??s suppliers. This is because cloud services often involve multiple parties in the supply chain, such as cloud providers, sub-providers, brokers, carriers, and auditors. Each party may have different roles and responsibilities in delivering the cloud services and ensuring their quality, security, and compliance. Therefore, it is essential for the client organization to have visibility and assurance of the performance and compliance of the provider??s suppliers
and to establish clear and transparent agreements with them regarding their roles, responsibilities, expectations, and obligations.12
An auditor should be aware of the importance of the client organization??s understanding of the provider??s suppliers because it provides a basis for assessing the risks and challenges associated with outsourcing services to a cloud provider and its supply chain. An auditor can use the client organization??s understanding of the provider??s suppliers to verify that the client organization has conducted a thorough due diligence of the provider??s suppliers and their capabilities, qualifications, certifications, and reputation. An auditor can also use the client organization??s understanding of the provider??s suppliers to evaluate whether the client organization has implemented adequate controls and processes to monitor, audit, or verify the security and compliance status of their cloud services and data across the supply chain. An auditor can also use the client organization??s understanding of the provider??s suppliers to identify any gaps or weaknesses in the client organization??s security management program and to provide recommendations for improvement.34
References := Practical Guide to Cloud Service Agreements Version 2.01; HIDDEN INTERDEPENDENCIES BETWEEN INFORMATION AND ORGANIZATIONAL ??2; Cloud
Computing: The Audit Challenge - ISACA3; Cloud Computing: Audit Considerations - AICPA4

NEW QUESTION 46
The three layers of Open Certification Framework (OCF) PRIMARILY help cloud service providers and cloud clients improve the level of:

A. legal and regulatory compliance.
B. risk and controls.
C. audit structure and formats.
D. transparency and assurance.

Answer: D

Explanation:
The three layers of the Open Certification Framework (OCF) primarily help cloud service providers and cloud clients improve the level of transparency and assurance. The OCF is designed to provide a trusted and independent evaluation of cloud providers through a flexible, incremental, and multi-layered certification process. This framework enhances transparency by making it easier for consumers to understand and compare providers?? security and compliance capabilities. Additionally, it offers assurance by integrating with third-party assessment and attestation statements, thereby increasing the security baseline for all participants.
References = The benefits of the OCF in improving transparency and assurance are
detailed in the Cloud Security Alliance??s documentation on the Open Certification Framework1.

NEW QUESTION 50
An auditor is reviewing an organization??s virtual machines (VMs) hosted in the cloud. The organization utilizes a configuration management (CM) tool to enforce password policies on its VMs. Which of the following is the BEST approach for the auditor to use to review the operating effectiveness of the password requirement?

A. The auditor should not rely on the CM tool and its settings, and for thoroughness shouldreview the password configuration on the set of sample VMs.
B. Review the relevant configuration settings on the CM tool and check whether the CM tool agents are operating effectively on the sample VMs.
C. As it is an automated environment, reviewing the relevant configuration settings on the CM tool would be sufficient.

D. Review the incident records for any incidents relating to brute force attacks or password compromise in the last 12 months and investigate whether the root cause of the incidents was due to in appropriate password policy configured on the VMs.

Answer: B

Explanation:
The best approach for an auditor to review the operating effectiveness of the password requirement is to review the configuration settings on the Configuration Management (CM) tool and verify that the CM tool agents are functioning correctly on the VMs. This method ensures that the password policies are being enforced as intended and that the CM tool is effectively managing the configurations across the organization??s virtual machines. It provides a balance between relying solely on automated tools and manual verification processes.
References = This approach is supported by best practices in cloud security and auditing, which recommend a combination of automated tools and manual checks to ensure the effectiveness of security controls123. The use of CM tools for enforcing password policies is a common practice, and their effectiveness must be regularly verified to maintain the security posture of cloud services.

NEW QUESTION 55
To promote the adoption of secure cloud services across the federal government by

A. To providing a standardized approach to security and risk assessment
B. To provide agencies of the federal government a dedicated tool to certify Authority to Operate (ATO)
C. To enable 3PAOs to perform independent security assessments of cloud service providers
D. To publish a comprehensive and official framework for the secure implementation of controls for cloud security

Answer: A

Explanation:
The correct answer is A. To providing a standardized approach to security and risk assessment. This is the main purpose of FedRAMP, which is a government-wide program that promotes the adoption of secure cloud services across the federal government. FedRAMP provides a standardized methodology for assessing, authorizing, and monitoring the security of cloud products and services, and enables agencies to leverage the security assessments of cloud service providers (CSPs) that have been approved by FedRAMP. FedRAMP also establishes a baseline set of security controls for cloud computing, based on NIST SP 800-53, and provides guidance and templates for implementing and documenting the controls1.
The other options are incorrect because:
? B. To provide agencies of the federal government a dedicated tool to certify Authority to Operate (ATO): FedRAMP does not provide a tool to certify ATO, but rather a process to obtain a provisional ATO (P-ATO) from the Joint Authorization Board (JAB) or an agency ATO from a federal agency. ATO is the official management decision given by a senior official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls2.
? C. To enable 3PAOs to perform independent security assessments of cloud
service providers: FedRAMP does not enable 3PAOs to perform independent security assessments of CSPs, but rather requires CSPs to use 3PAOs for conducting independent security assessments as part of the FedRAMP
process. 3PAOs are independent entities that have been accredited by FedRAMP to perform initial and periodic security assessments of CSPs?? systems and provide evidence of compliance with FedRAMP requirements3.
? D. To publish a comprehensive and official framework for the secure
implementation of controls for cloud security: FedRAMP does not publish a comprehensive and official framework for the secure implementation of controls for cloud security, but rather adopts and adapts the existing framework of NIST SP 800-53, which provides a catalog of security and privacy controls for federal information systems and organizations. FedRAMP tailors the NIST SP 800-53 controls to provide a subset of controls that are specific to cloud computing, and categorizes them into low, moderate, and high impact levels based on FIPS 1994.
References:
? Learn What FedRAMP is All About | FedRAMP | FedRAMP.gov
? Guide for Applying the Risk Management Framework to Federal Information Systems - NIST
? Third Party Assessment Organizations (3PAO) | FedRAMP.gov
? Security and Privacy Controls for Federal Information Systems and Organizations - NIST

NEW QUESTION 57
Which of the following has the MOST substantial impact on how aggressive or conservative the cloud approach of an organization will be?

A. Applicable laws and regulations
B. Internal policies and technical standards
C. Risk scoring criteria
D. Risk appetite and budget constraints

Answer: D

Explanation:
Risk appetite and budget constraints have the most substantial impact on how aggressive or conservative the cloud approach of an organization will be. Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. Budget constraints are the limitations on the financial resources that an organization can allocate to its cloud initiatives. Both factors influence the organization??s strategic decisions on which cloud service models, deployment models, providers, and solutions to adopt, as well as the level of security, compliance, and performance to achieve. An organization with a high risk appetite and a large budget may opt for a more aggressive cloud approach, such as moving critical applications and data to a public cloud provider, while an organization with a low risk appetite and a small budget may opt for a more conservative cloud approach, such as keeping sensitive information on-premises or using a private cloud provider12.
References:
? ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 17- 18.
? CSA, Cloud Controls Matrix (CCM) v4.0, 2021, p. 63.

NEW QUESTION 61
Which of the following types of SOC reports BEST helps to ensure operating effectiveness of controls in a cloud service provider offering?

A. SOC 3 Type 2
B. SOC 2 Type 2
C. SOC 1 Type 1
D. SOC 2 Type 1

Answer: B

Explanation:
A SOC 2 Type 2 report is the most comprehensive type of report for cloud service providers, as it evaluates the design and operating effectiveness of a service organization??s controls over a period of time. This type of report is specifically intended to meet the needs of customers who need assurance about the security, availability, processing integrity, confidentiality, or privacy of the data processed by the service provider1234.
References = The importance of SOC 2 Type 2 reports for cloud service providers is discussed in various resources, including those provided by ISACA and the Cloud Security Alliance, which highlight the need for such reports to ensure the operating effectiveness of controls5678.

NEW QUESTION 65
Which of the following is the MOST important audit scope document when conducting a review of a cloud service provider?

A. Processes and systems to be audited
B. Updated audit work program
C. Documentation criteria for the audit evidence
D. Testing procedure to be performed

Answer: A

Explanation:
According to the definition of audit scope, it is the extent and boundaries of an audit, which include the audit objectives, the activities and documents covered, the time period and locations audited, and the related activities not audited1 Audit scope determines how deeply an audit is performed and may vary depending on the type of audit. Audit scope can also mean the examination of a person or the inspection of the books, records, or accounts of a person for tax purposes1
The most important audit scope document when conducting a review of a cloud service provider is the processes and systems to be audited. This document defines the specific areas and aspects of the cloud service provider that will be subject to the audit, such as the cloud service delivery model, the cloud deployment model, the cloud security domains, the cloud service level agreements, the cloud governance framework, etc2 The processes and systems to be audited document also helps to identify the risks, controls, criteria, and objectives of the audit, as well as the roles and responsibilities of the auditors and the auditees3 The processes and systems to be audited document is essential for planning and performing an effective and efficient audit of a cloud service provider.
The other options are not correct because:
? Option B is not correct because the updated audit work program is not an audit scope document, but rather an audit planning document. The audit work program is a set of detailed instructions or procedures that guide the auditor in conducting the audit activities4 The audit work program is based on the audit scope, but it does not define it. The audit work program may also change during the course of the audit, depending on the findings and issues encountered by the auditor4
? Option C is not correct because the documentation criteria for the audit evidence is not an audit scope document, but rather an audit quality document. The documentation criteria for the audit evidence is a set of standards or guidelines that specify what constitutes sufficient and appropriate evidence to support the auditor??s conclusions and opinions5 The documentation criteria for the audit evidence is derived from the audit scope, but it does not determine it. The documentation criteria for the audit evidence may also vary depending on the nature and source of the evidence collected by the auditor5
? Option D is not correct because the testing procedure to be performed is not an audit scope document, but rather an audit execution document. The testing procedure to be performed is a set of steps or actions that describe how to test or verify a specific control or process within the cloud service provider6 The testing procedure to be performed is aligned with the audit scope, but it does not establish it. The testing procedure to be performed may also differ depending on the type and level of testing required by the auditor6
References: 1: AUDIT SCOPE DEFINITION - VentureLine 2: Audit Scope and Criteria - Auditor Training Online 3: Open Certification Framework | CSA - Cloud Security Alliance 4: Audit Work Program Definition - Audit Work Program Example 5: INTERNATIONAL STANDARD ON AUDITING 230 AUDIT DOCUMENTATION CONTENTS - IFAC 6: What
are Testing Procedures? - Definition from Techopedia

NEW QUESTION 66
When an organization is moving to the cloud, responsibilities are shared based upon the cloud service provider's model and accountability is:

A. shared.
B. avoided.
C. transferred.
D. maintained.

Answer: D

Explanation:
When an organization is moving to the cloud, responsibilities are shared based upon the cloud service provider??s model and accountability is maintained. This means that the organization remains accountable for the security and compliance of its data and applications in the cloud, even if some of the security responsibilities are delegated to the cloud service provider (CSP). The organization cannot transfer or avoid its accountability to the CSP or any other third party, as it is ultimately responsible for its own business outcomes, legal obligations, and reputation. Therefore, the organization must understand the shared responsibility model and which security tasks are handled by the CSP and which tasks are handled by itself. The organization must also monitor and audit the CSP??s performance and security, and mitigate any risks or issues that may arise12. References:
? Shared responsibility in the cloud - Microsoft Azure
? Understanding the Shared Responsibilities Model in Cloud Services - ISACA

NEW QUESTION 68
The PRIMARY purpose of Open Certification Framework (OCF) for the CSA STAR program is to:

A. facilitate an effective relationship between the cloud service provider and cloud client.
B. ensure understanding of true risk and perceived risk by the cloud service users.
C. provide global, accredited, and trusted certification of the cloud service provider.
D. enable the cloud service provider to prioritize resources to meet its own requirements.

Answer: C

Explanation:
According to the CSA website, the primary purpose of the Open Certification Framework (OCF) for the CSA STAR program is to provide global, accredited, trusted certification of cloud providers1 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 framework2 The OCF aims to address the gaps within the IT ecosystem that are inhibiting market adoption of secure and reliable cloud services, such

as the lack of simple, cost effective ways to evaluate and compare providers?? resilience, data protection, privacy, and service portability2 The OCF also aims to promote industry transparency and reduce complexity and costs for both providers and customers3
The other options are not correct because:
? Option A is not correct because facilitating an effective relationship between the cloud service provider and cloud client is not the primary purpose of the OCF for the CSA STAR program, but rather a potential benefit or outcome of it. The OCF can help facilitate an effective relationship between the provider and the client by providing a common language and framework for assessing and communicating the security and compliance posture of the provider, as well as enabling trust and confidence in the provider??s capabilities and performance. However, this is not the main goal or objective of the OCF, but rather a means to achieve it.
? Option B is not correct because ensuring understanding of true risk and perceived risk by the cloud service users is not the primary purpose of the OCF for the CSA STAR program, but rather a possible implication or consequence of it. The OCF can help ensure understanding of true risk and perceived risk by the cloud service users by providing objective and verifiable information and evidence about the provider??s security and compliance level, as well as allowing comparison and benchmarking with other providers in the market. However, this is not the main aim or intention of the OCF, but rather a result or effect of it.
? Option D is not correct because enabling the cloud service provider to prioritize resources to meet its own requirements is not the primary purpose of the OCF for the CSA STAR program, but rather a potential advantage or opportunity for it. The OCF can enable the cloud service provider to prioritize resources to meet its own requirements by providing a flexible, incremental and multi-layered approach to certification and/or attestation that allows the provider to choose the level of assurance that suits their business needs and goals. However, this is not the main reason or motivation for the OCF, but rather a benefit or option for it.
References: 1: Open Certification Framework Working Group | CSA 2: Open Certification Framework | CSA - Cloud Security Alliance 3: Why your cloud services need the CSA STAR Registry listing

NEW QUESTION 72
As Infrastructure as a Service (laaS) cloud service providers often do not allow the cloud service customers to perform on-premise audits, the BEST approach for the auditor should be to:

A. use other sources of available data for evaluating the customer's controls.
B. recommend that the customer not use the services provided by the provider.
C. refrain from auditing the provider's security controls due to lack of cooperation.
D. escalate the lack of support from the provider to the regulatory authority.

Answer: A

Explanation:
In situations where Infrastructure as a Service (IaaS) cloud service providers do not permit on-premise audits, auditors must adapt by utilizing alternative sources of data to evaluate the customer??s controls. This can include using automated tools, third-party certifications, and other forms of assurance provided by the service provider. This approach ensures that the auditor can still assess the security posture and compliance of the cloud services without direct physical access to the provider??s infrastructure. References = The Cloud Security Alliance (CSA) provides guidelines on effective cloud auditing practices, including the use of alternative data sources when on-premise audits are not feasible1. Additionally, discussions on the Certificate of Cloud Auditing Knowledge (CCAK) highlight the importance of adapting audit strategies to the cloud environment2.

NEW QUESTION 76
Which of the following is MOST useful for an auditor to review when seeking visibility into the cloud supply chain for a newly acquired Software as a Service (SaaS) solution?

A. SaaS provider contract
B. Payments made by the service owner
C. SaaS vendor white papers
D. Cloud compliance obligations register

Answer: A

Explanation:
The most useful document for an auditor to review when seeking visibility into the cloud supply chain for a newly acquired Software as a Service (SaaS) solution is the SaaS provider contract. The contract is the legal agreement that defines the terms and conditions of the cloud service, including the roles, responsibilities, and obligations of the parties involved1. The contract should also specify the service level agreements (SLAs), security and privacy requirements, data ownership and governance, incident response and reporting, audit rights and access, and subcontracting or outsourcing arrangements of the SaaS provider2. By reviewing the contract, the auditor can gain insight into the cloud supply chain and assess the risks, controls, and compliance of the SaaS solution.
The other options are not as useful as the SaaS provider contract. Payments made by the service owner are the financial transactions that reflect the fees or charges incurred by using the SaaS solution. They may indicate the usage or consumption of the cloud service, but they do not provide much information about the cloud supply chain or its security and compliance aspects3. SaaS vendor white papers are the marketing or educational materials that describe the features, benefits, or best practices of the SaaS solution. They may provide some general or technical information about the cloud service, but they are not legally binding or verifiable4. Cloud compliance obligations register is a tool that helps customers identify and track their compliance requirements and obligations for using cloud services. It may help customers understand their own responsibilities and risks in relation to the cloud service, but it does not necessarily reflect the compliance status or performance of the SaaS provider5.
References:
? Cloud Services Due Diligence Checklist | Trust Center1, section on How to use the checklist
? Cloud Computing Security Considerations | Cyber.gov.au2, section on Contractual arrangements
? Cloud Computing Pricing Models: A Comparison - DZone Cloud3, section on Pricing Models
? What is a White Paper? Definition from WhatIs.com4, section on White Paper
? Cloud Compliance Obligations Register | Cyber.gov.au5, section on Cloud Compliance Obligations Register

NEW QUESTION 80
Which of the following is a category of trust in cloud computing?

A. Loyalty-based trust
B. Background-based trust
C. Reputation-based trust
D. Transparency-based trust

Answer: C

Explanation:
Reputation-based trust is a category of trust in cloud computing that relies on the feedback, ratings, reviews, or recommendations of other users or third parties

who have used or evaluated the cloud service provider or the cloud service. Reputation-based trust reflects the collective opinion and experience of the cloud community regarding the quality, reliability, security, and performance of the cloud service provider or the cloud service. Reputation-based trust can help potential customers to make informed decisions about choosing a cloud service provider or a cloud service based on the reputation score or
ranking of the provider or the service. Reputation-based trust can also motivate cloud service providers to improve their services and maintain their reputation by meeting or exceeding customer expectations.

Reputation-based trust is one of the most common and widely used forms of trust in cloud computing, as it is easy to access and understand. However, reputation-based trust also has some limitations and challenges, such as:

? The accuracy and validity of the reputation data may depend on the source, method, and frequency of data collection and aggregation. For example, some reputation data may be outdated, incomplete, biased, manipulated, or falsified by malicious actors or competitors.

? The interpretation and comparison of the reputation data may vary depending on the context, criteria, and preferences of the customers. For example, some customers may value different aspects of the cloud service more than others, such as security, availability, cost, or functionality.

? The trustworthiness and accountability of the reputation system itself may be questionable. For example, some reputation systems may lack transparency, consistency, or standardization in their design, implementation, or operation.

Therefore, reputation-based trust should not be the only factor for trusting a cloud service provider or a cloud service. Customers should also consider other forms of trust in cloud computing, such as evidence-based trust, policy-based trust, or certification-based trust

NEW QUESTION 83

A business unit introducing cloud technologies to the organization without the knowledge or approval of the appropriate governance function is an example of:

A. IT exception
B. Threat
C. Shadow IT
D. Vulnerability

Answer: C

Explanation:

Shadow IT refers to the use of IT resources (hardware, software, or cloud services) within an organization without the explicit approval of the IT or governance team. This practice is often flagged in cloud audits due to potential risks of compliance violations and security threats. The CCAK documentation from ISACA highlights the need for visibility and governance over all IT assets, with specific controls listed in the CSA CCM for Cloud Governance (GOV-09). Shadow IT poses risks to data security, compliance, and can introduce vulnerabilities, as systems are not subject to organizational standards and oversight.

========================

NEW QUESTION 87

Cloud Controls Matrix (CCM) controls can be used by cloud customers to:

A. develop new security baselines for the industry.
B. define different control frameworks for different cloud service providers.
C. build an operational cloud risk management program.
D. facilitate communication with their legal department.

Answer: C

Explanation:

The Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing that can be used by cloud customers to build an operational cloud risk management program. The CCM provides guidance on which security controls should be implemented by which actor within the cloud supply chain, and maps the controls to industry-accepted security standards, regulations, and frameworks. The CCM can help cloud customers to assess the security posture of their cloud service providers, document their own responsibilities and requirements, and establish a baseline for cloud security assurance and compliance. References :=

? Cloud Controls Matrix (CCM) - CSA1

? What is the Cloud Controls Matrix (CCM)? - Cloud Security Alliance2

? Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, Chapter 5: Cloud Assurance Frameworks

NEW QUESTION 90

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?

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 features1 It involves re-running functional and non-functional tests to ensure that previously developed and tested software still performs as expected after a change2 Regression 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 time4 Parallel 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 performance6 Full 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.
References: 1: Wikipedia. Regression testing - Wikipedia. [Online]. Available: 3. [Accessed: 14-Apr-2023]. 2: Katalon. What is Regression Testing? Definition, Tools, Examples -
Katalon. [Online]. Available: 4. [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: Guru99. What is Parallel Testing? with Example - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023]. 5: LambdaTest. Parallel Testing In Selenium WebDriver | LambdaTest Blog. [Online]. Available: . [Accessed: 14-
Apr-2023]. 6: Guru99. What is Unit Testing? Types & Examples - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023]. 7: Software Testing Help. Unit Testing Vs Integration Testing: Difference Between These Two - SoftwareTestingHelp.com Blog. [Online].
Available: . [Accessed: 14-Apr-2023]. : Guru99. What is Functional Testing? Types & Examples - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023]. : Software Testing Help. Functional Testing Vs Non-Functional Testing - SoftwareTestingHelp.com Blog.
[Online]. Available: . [Accessed: 14-Apr-2023].

NEW QUESTION 91
Which of the following key stakeholders should be identified FIRST when an organization is designing a cloud compliance program?

A. Cloud strategy owners
B. Internal control function
C. Cloud process owners
D. Legal functions

Answer: A

Explanation:
When designing a cloud compliance program, the first key stakeholders to identify are the cloud strategy owners. These individuals or groups are responsible for the overarching direction and objectives of the cloud initiatives within the organization. They play a crucial role in aligning the compliance program with the business goals and ensuring that the cloud services are used effectively and in compliance with relevant laws and regulations. By starting with the cloud strategy owners, an organization ensures that the compliance program is built on a foundation that supports the strategic vision and provides clear guidance for all subsequent compliance-related activities and decisions.
References = The information provided is based on general best practices for cloud compliance and stakeholder management. Specific references from the Cloud Auditing Knowledge (CCAK) documents and related resources by ISACA and the Cloud Security Alliance (CSA) are not directly cited here, as my current capabilities do not include accessing or verifying content from external documents or websites. However, the answer aligns with the recognized approach of prioritizing strategic leadership in the initial stages of designing a compliance program.

NEW QUESTION 92
The control domain feature within a Cloud Controls Matrix (CCM) represents:

A. CCM's ability to scan and check Active Directory, LDAP, and x.500 directories for suspicious and/or privileged user accounts.
B. a logical grouping of security controls addressing the same category of IT risks or information security concerns.
C. a set of application programming interfaces (APIs) that allows a cloud consumer to restrict the replication area within a well-defined jurisdictional perimeter.
D. CCM's ability to scan for anomalies in DNS zones in order to detect DNS spoofing, DNS hijacking, DNS cache poisoning, and similar threats.

Answer: B

NEW QUESTION 93
To BEST prevent a data breach from happening, cryptographic keys should be:

A. distributed in public-facing repositories.
B. embedded in source code.
C. rotated regularly.
D. transmitted in clear text.

Answer: C

Explanation:
Rotating cryptographic keys regularly is a security best practice that helps to mitigate the risk of unauthorized access to encrypted data. When keys are rotated, old keys are retired and replaced with new ones, making any compromised keys useless to an attacker. This process helps to limit the time window during which a stolen key can be used to breach data. Key rotation is a fundamental aspect of key management lifecycle best practices, which include generating new key pairs, rotating keys at set intervals, revoking access to keys, and destroying out-of-date or compromised keys.
References = The importance of key rotation is supported by various security standards and best practices, including recommendations from the National Institute of Standards and Technology (NIST)1 and the Cloud Security Alliance (CSA)23. These sources emphasize the need for periodic renewal and decommissioning of old keys as part of a comprehensive key management strategy.

NEW QUESTION 97
"Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls." Which of the following types of controls BEST matches this control description?

A. Virtual instance and OS hardening
B. Network security
C. Network vulnerability management
D. Change detection

Answer: B

Explanation:
The correct answer is B. Network security is the type of control that best matches the control description given in the question. Network security involves designing and configuring network environments and virtual instances to restrict and monitor traffic between trusted and untrusted connections, such as firewalls, routers, switches, VPNs, and network segmentation. Network security also requires periodic reviews and documentation of the network configurations and the justification for the allowed services, protocols, ports, and compensating controls.

The other options are not directly related to the question. Option A, virtual instance and OS hardening, refers to the process of applying security configurations and patches to virtual instances and operating systems to reduce their attack surface and vulnerabilities. Option C, network vulnerability management, refers to the process of identifying, assessing, prioritizing, and remediating network vulnerabilities using tools such as scanners, analyzers, and testers. Option D, change detection, refers to the process of monitoring and detecting changes in the system or network environment that could affect the security posture or performance of the system or network.
References :=
? IVS-01: Network Security - CSF Tools - Identity Digital1
? Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, Chapter 6: Cloud Security Controls
? Cloud Controls Matrix (CCM) - CSA2

NEW QUESTION 101
The CSA STAR Certification is based on criteria outlined the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) in addition to:

A. ISO/IEC 27001 implementation.
B. GB/T 22080-2008.
C. SOC 2 Type 1 or 2 reports.
D. GDPR CoC certification.

Answer: A

Explanation:
The CSA STAR Certification is based on criteria outlined in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) in addition to ISO/IEC 27001 implementation. ISO/IEC 27001 is an international standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). The CSA STAR Certification is a third-party independent assessment of the security of a cloud service provider, which demonstrates the alignment of the provider??s ISMS with the CCM best practices. The CSA STAR Certification has three levels: Level 1 (STAR Certification), Level 2 (STAR Attestation), and
Level 3 (STAR Continuous Monitoring).1 [2][2] References := CCAK Study Guide, Chapter 5: Cloud Auditing, page 971; CSA STAR Certification, Overview[2][2]

NEW QUESTION 102
Which of the following methods can be used by a cloud service provider with a cloud customer that does not want to share security and control information?

A. Nondisclosure agreements (NDAs)
B. Independent auditor report
C. First-party audit
D. Industry certifications

Answer: B

Explanation:
An independent auditor report is a method that can be used by a cloud service provider (CSP) with a cloud customer that does not want to share security and control information. An independent auditor report is a document that provides assurance on the CSP??s security and control environment, based on an audit conducted by a qualified third-party auditor. The audit can be based on various standards or frameworks, such as ISO 27001, SOC 2, CSA STAR, etc. The independent auditor report can provide the cloud customer with the necessary information to evaluate the CSP??s security and control posture, without disclosing sensitive or proprietary details. The CSP can also use the independent auditor report to demonstrate compliance with relevant regulations or contractual obligations.
References:
? ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 83- 84.
? ISACA, Cloud Computing Audit Program, 2019, p. 6-7.

NEW QUESTION 103
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
What should be the BEST recommendation to reduce the provider??s burden?

A. The provider can answer each customer individually.
B. The provider can direct all customer inquiries to the information in the CSA STAR registry.
C. The provider can schedule a call with each customer.
D. The provider can share all security reports with customers to streamline the process

Answer: B

Explanation:
The CSA STAR registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings. The registry is based on the Cloud Controls Matrix (CCM), which is a framework of cloud-specific security best practices, and the GDPR Code of Conduct, which is a set of privacy principles for cloud service providers. The registry allows cloud customers to assess the security and compliance posture of cloud service providers, as well as to compare different providers based on their level of assurance. The registry also reduces the complexity and cost of filling out multiple customer questionnaires and requests for proposal (RFPs). Therefore, the best recommendation to reduce the provider??s burden is to direct all customer inquiries to the information in the CSA STAR registry, which can demonstrate the provider??s transparency, trustworthiness, and adherence to industry standards. The provider can also encourage customers to use the Consensus Assessments Initiative Questionnaire (CAIQ), which is a standardized set of questions based on the CCM, to evaluate the provider??s security controls. Alternatively, the provider can pursue higher levels of assurance, such as third-party audits or continuous monitoring, to further validate their security and privacy practices and increase customer confidence.
References:
? STAR Registry | CSA
? STAR | CSA
? CSA Security Trust Assurance and Risk (STAR) Registry Reaches Notable ??
? Why CSA STAR Is Important for Cloud Service Providers - A-LIGN

NEW QUESTION 106
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?

A. ISAE 3402 report
B. ISO/IEC 27001 certification
C. SOC1 Type 1 report
D. SOC2 Type 2 report

Answer: D

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 109
When reviewing a third-party agreement with a cloud service provider, which of the following should be the GREATEST concern regarding customer data privacy?

A. Return or destruction of information
B. Data retention, backup, and recovery
C. Patch management process
D. Network intrusion detection

Answer: A

Explanation:
When reviewing a third-party agreement with a cloud service provider, the greatest concern regarding customer data privacy is the return or destruction of information. This is because customer data may contain sensitive or personal information that needs to be protected from unauthorized access, use, or disclosure. The cloud service provider should have clear and transparent policies and procedures for returning or destroying customer data upon termination of the agreement or upon customer request. The cloud service provider should also provide evidence of the return or destruction of customer data, such as certificates of destruction, audit logs, or reports. The return or destruction of information should comply with applicable laws and regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or the Health Insurance Portability and Accountability Act (HIPAA). The cloud service provider should also ensure that any subcontractors or affiliates that have access to customer data follow the same policies and procedures12.
References:
? Cloud Services Agreements – Protecting Your Hosted Environment
? CSP agreements, price lists, and offers - Partner Center

NEW QUESTION 113
When developing a cloud compliance program, what is the PRIMARY reason for a cloud customer

A. To determine the total cost of the cloud services to be deployed
B. To confirm whether the compensating controls implemented are sufficient for the cloud services
C. To determine how those services will fit within its policies and procedures
D. To confirm which vendor will be selected based on compliance with security requirements

Answer: C

Explanation:
When developing a cloud compliance program, the primary reason for a cloud customer to determine how those services will fit within its policies and procedures is to ensure that the cloud services are aligned with the customer??s business objectives, risk appetite, and compliance obligations. Cloud services may have different characteristics, features, and capabilities than traditional on-premises services, and may require different or additional controls to meet the customer??s security and compliance requirements. Therefore, the customer needs to assess how the cloud services will fit within its existing policies and procedures, such as data classification, data protection, access management, incident response, audit, and reporting. The customer also needs to identify any gaps or conflicts between the cloud services and its policies and procedures, and implement appropriate measures to address them. By doing so, the customer can ensure that the cloud services are used in a secure, compliant, and effective manner12.
References:
? ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 19- 20.
? Cloud Compliance Frameworks: What You Need to Know

NEW QUESTION 116
During the planning phase of a cloud audit, the PRIMARY goal of a cloud auditor is to:

A. specify appropriate tests.
B. address audit objectives.
C. minimize audit resources.
D. collect sufficient evidence.

Answer: B

Explanation:
According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, the primary goal of a cloud auditor during the planning phase of a cloud audit is to address audit objectives1. The audit objectives are the specific questions that the audit aims to answer, such as whether the cloud service meets the security, compliance, performance, and availability requirements of the cloud customer. The audit objectives should be aligned with the organization??s context, risk appetite, and expectations. The audit objectives should also be clear, measurable, achievable, relevant, and timely.
The other options are not the primary goal of a cloud auditor during the planning phase of a cloud audit. Option A is a possible activity, but not the main goal of the planning phase. The appropriate tests are determined based on the audit objectives, criteria, and methodology. Option C is a possible constraint, but not the main

goal of the planning phase. The audit resources should be allocated based on the audit scope, complexity, and significance. Option D is a possible outcome, but not the main goal of the planning phase. The sufficient evidence is collected during the execution phase of the audit, based on the audit plan. References:
? ISACA Cloud Auditing Knowledge Certificate Study Guide, page 12-13.

NEW QUESTION 121
Which of the following is a PRIMARY benefit of using a standardized control framework?

A. It enables senior management to receive regular and detailed executive reports easily.
B. It enables the organization to implement an effective process of control measurement.
C. It enables auditors to assess an information system based on a well-defined set of controls.
D. It enables consultants to speed up the implementation of management systems, thus reducing costs.

Answer: C

NEW QUESTION 122
A cloud service provider utilizes services of other service providers for its cloud service. Which of the following is the BEST approach for the auditor while performing the audit for the cloud service?

A. The auditor should review the service providers' security controls even more strictly, as they are further separated from the cloud customer.
B. The auditor should review the relationship between the cloud service provider and its service provider to help direct and estimate the level of effort and analysis the auditor should apply.
C. As the contract for the cloud service is between the cloud customer and the cloud service provider, there is no need for the auditor to review the services provided by the service providers.
D. As the relationship between the cloud service provider and its service providers is governed by separate contracts between them, there is no need for the auditor to review the services

Answer: B

Explanation:
According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, the auditor should review the relationship between the cloud service provider and its service provider to help direct and estimate the level of effort and analysis the auditor should apply1. The auditor should understand the nature and scope of the services provided by the service provider, the contractual obligations and service level agreements, the security and compliance requirements, and the monitoring and reporting mechanisms.
The auditor should also assess the risks and controls associated with the service provider, and determine if additional audit procedures are needed to obtain sufficient assurance. The other options are not the best approach for the auditor. Option A is too strict and might not be feasible or necessary, depending on the type and level of services provided by the service provider. Option C is too lax and might overlook significant risks and gaps in the cloud service. Option D is too narrow and might ignore the impact of the service provider on the cloud customer??s business context. References:
? ISACA Cloud Auditing Knowledge Certificate Study Guide, page 13-14.

NEW QUESTION 125
If a customer management interface is compromised over the public Internet, it can lead to:

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.
References:
? 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

NEW QUESTION 126
To ensure that compliance obligations for data residency in the cloud are aligned with an organization's risk appetite, which of the following activities is MOST important to perform?

A. Manage compliance obligations through a structured risk management process.
B. Communicate the organization's risk appetite across cloud service providers.
C. Perform a cloud vendor assessment every time there is a change to data flows.
D. Develop risk metrics to show how the organization is meeting the obligations.

Answer: A

NEW QUESTION 130
What type of termination occurs at the initiative of one party and without the fault of the other party?

A. Termination without the fault
B. Termination at the end of the term
C. Termination for cause
D. Termination for convenience

Answer: D

Explanation:
Termination for convenience is a contractual provision that allows one party to unilaterally terminate the contract without the fault of the other party. This type of termination does not require the terminating party to prove that the other party has failed to meet their obligations or is at fault in any way. Instead, it is often used to end a contract when it is no longer in the best interest of the terminating party to continue, for reasons that may include changes in business strategy, financial considerations, or other external factors.
References = The concept of termination for convenience is commonly found in various contractual agreements and is a standard clause in government contracts, allowing the government to terminate a contract when it is deemed to be in the public interest. While the search did not yield specific CCAK documents detailing this type of termination, it is a well-established principle in contract law and is likely covered under the broader topic of contract management within the CCAK curriculum.

NEW QUESTION 134
What aspect of Software as a Service (SaaS) functionality and operations would the cloud customer be responsible for and should be audited?

A. Access controls
B. Vulnerability management
C. Patching
D. Source code reviews

Answer: A

Explanation:
According to the cloud shared responsibility model, the cloud customer is responsible for managing the access controls for the SaaS functionality and operations, and this should be audited by the cloud auditor12. Access controls are the mechanisms that restrict and regulate who can access and use the SaaS applications and data, and how they can do so. Access controls include identity and access management, authentication, authorization, encryption, logging, and monitoring. The cloud customer is responsible for defining and enforcing the access policies, roles, and permissions for the SaaS users, as well as ensuring that the access controls are aligned with the security and compliance requirements of the customer??s business context12.
The other options are not the aspects of SaaS functionality and operations that the cloud customer is responsible for and should be audited. Option B is incorrect, as vulnerability management is the process of identifying, assessing, and mitigating the security weaknesses in the SaaS applications and infrastructure, and this is usually handled by the cloud service provider12. Option C is incorrect, as patching is the process of updating and fixing the SaaS applications and infrastructure to address security issues or improve performance, and this is also usually handled by the cloud service provider12. Option D is incorrect, as source code reviews are the process of examining and testing the SaaS applications?? source code to detect errors or vulnerabilities, and this is also usually handled by the cloud service provider12. References:
? Shared responsibility in the cloud - Microsoft Azure
? The Customer??s Responsibility in the Cloud Shared Responsibility Model - ISACA

NEW QUESTION 139
Which of the following can be used to determine whether access keys are stored in the source code or any other configuration files during development?

A. Static code review
B. Dynamic code review
C. Vulnerability scanning
D. Credential scanning

Answer: D

Explanation:
Credential scanning is a technique that can be used to detect and prevent the exposure of access keys and other sensitive information in the source code or any other configuration files during development. Credential scanning tools can scan the code repositories, files, and commits for any hardcoded credentials, such as access keys, passwords, tokens, certificates, and connection strings. They can also alert the developers or security teams of any potential leaks and suggest remediation actions, such as rotating or revoking the compromised keys, removing the credentials from the code, or using secure storage mechanisms like vaults or environment variables. Credential scanning can be integrated into the development pipeline as part of the continuous integration and continuous delivery (CI/CD) process, or performed periodically as a security audit. Credential scanning can help reduce the risk of credential leakage, which can lead to unauthorized access, data breaches, or account compromise. References:
? Protecting Source Code in the Cloud with DSPM
? Best practices for managing service account keys
? Protect your code repository

NEW QUESTION 142
Which plan guides an organization on how to react to a security incident that might occur on the organization's systems, or that might be affecting one of its service providers?

A. Incident response plan
B. Security incident plan
C. Unexpected event plan
D. Emergency incident plan

Answer: A

NEW QUESTION 146
What is an advantage of using dynamic application security testing (DAST) over static application security testing (SAST) methodology?

A. DAST is slower but thorough.
B. Unlike SAST, DAST is a black box and programming language agnostic.
C. DAST can dynamically integrate with most continuous integration and continuous delivery (CI/CD) tools.
D. DAST delivers more false positives than SAST

Answer: B

Explanation:
Dynamic application security testing (DAST) is a method of testing the security of an application by simulating attacks from an external source. DAST does not require access to the source code or binaries of the application, unlike static application security testing (SAST), which analyzes the code for vulnerabilities. Therefore, DAST is a black box testing technique, meaning that it does not need any knowledge of the internal structure, design, or implementation of the application. DAST is also programming language agnostic, meaning that it can test applications written in any language, framework, or platform. This makes DAST more flexible and adaptable to different types of applications and environments. However, DAST also has some limitations, such as being slower, less accurate, and more dependent on the availability and configuration of the application. References:
? SAST vs. DAST: What??s the Difference?
? SAST vs DAST: What??s the Difference?
? SAST vs. DAST: Enhancing application security

NEW QUESTION 149
A cloud service provider 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 provider's security operation center is not notified in advance of the scope of the audit and the test vectors. Which mode has been selected by the provider?

A. Reversal
B. Double blind
C. Double gray box
D. Tandem

Answer: B

Explanation:
A double blind penetration test is a type of pen test where the hacker has no prior knowledge of the target??s defenses, assets, or channels, and the target??s security team is not notified in advance of the scope of the audit and the test vectors. This mode simulates a real-world attack scenario, where both the attacker and the defender have to rely on their skills and resources to achieve their objectives. A double blind penetration test can help evaluate the effectiveness of the target??s security posture, detection and response capabilities, and incident management procedures12.
References:
? What is Penetration Testing | Step-By-Step Process & Methods | Imperva
? 7 Types of Penetration Testing: Guide to Pentest Methods & Types

NEW QUESTION 152
Controls mapping found in the Scope Applicability column of the Cloud Controls Matrix (CCM) may help organizations to realize cost savings:

A. by avoiding duplication of efforts in the compliance evaluation and for the eventual control design and implementation.
B. by implementing layered security, thus reducing the likelihood of data breaches and the associated costs.
C. by avoiding the need to hire a cloud security specialist to perform the periodic risk assessment exercise.
D. by avoiding fines for breaching those regulations that impose a controls mapping in order to prove compliance

Answer: A

Explanation:
Controls mapping found in the Scope Applicability column of the Cloud Controls Matrix (CCM) may help organizations to realize cost savings by avoiding duplication of efforts in the compliance evaluation and for the eventual control design and implementation. The Scope Applicability column is a feature of the CCM that indicates which cloud model type (IaaS, PaaS, SaaS) or cloud environment (public, hybrid, private) a control applies to. This feature can help organizations to identify and select the most relevant and appropriate controls for their specific cloud scenario, as well as to map them
to multiple industry-accepted security standards, regulations, and frameworks. By doing so, organizations can reduce the time, resources, and costs involved in achieving and maintaining compliance with various cloud security requirements123.
The other options are not directly related to the question. Option B, by implementing layered security, thus reducing the likelihood of data breaches and the associated costs, is not a valid reason because layered security is a general principle of defense in depth, not a specific feature of the CCM or the Scope Applicability column. Option C, by avoiding the need to hire a cloud security specialist to perform the periodic risk assessment exercise, is not a valid reason because using the CCM or the Scope Applicability column does not eliminate the need for a cloud security specialist or a periodic risk assessment exercise, which are essential for ensuring the effectiveness and adequacy of the cloud security controls. Option D, by avoiding fines for breaching those regulations that impose a controls mapping in order to prove compliance, is not a valid reason because controls mapping is not a mandatory requirement for proving compliance, but a voluntary tool for facilitating compliance. References :=
? What is CAIQ? | CSA - Cloud Security Alliance1
? Understanding the Cloud Control Matrix | CloudBolt Software2
? Cloud Controls Matrix (CCM) - CSA

NEW QUESTION 156
The MAIN difference between the Cloud Controls Matrix (CCM) and the Consensus Assessment Initiative Questionnaire (CAIQ) is that:

A. CCM assesses the presence of controls, whereas CAIQ assesses the overall security of a service.
B. CCM has 14 domains, whereas CAIQ has 16 domains.
C. CCM provides a controls framework, whereas CAIQ provides industry-accepted ways to document which security controls exist in Infrastructure as a Service (laaS), Platform as a Service (PaaS), and Software as a Service (SaaS) offerings.
D. CCM has a set of security questions, whereas CAIQ has a set of security controls.

Answer: C

NEW QUESTION 159
Who should define what constitutes a policy violation?

A. The external auditor
B. The organization
C. The Internet service provider (ISP)
D. The cloud provider

Answer: B

Explanation:
The organization should define what constitutes a policy violation. A policy violation refers to the breach or violation of a written policy or rule of the organization. A policy or rule is a statement that defines the expectations, standards, or requirements for the behavior, conduct, or performance of the organization??s members, such as employees, customers, partners, or suppliers. Policies and rules can be based on various sources, such as laws, regulations, contracts, agreements, principles, values, ethics, or best practices12.
The organization should define what constitutes a policy violation because it is responsible for establishing, communicating, enforcing, and monitoring its own policies and rules. The organization should also define the consequences and remedies for policy violations, such as warnings, sanctions, penalties, termination, or legal action. The organization should ensure that its policies and rules are clear, consistent, fair, and aligned with its mission, vision, and goals12.
The other options are not correct. Option A, the external auditor, is incorrect because the external auditor is an independent party that provides assurance or verification of the organization??s financial statements, internal controls, compliance status, or performance. The external auditor does not define the organization??s policies and rules, but evaluates them against relevant standards or criteria3. Option C, the Internet service provider (ISP), is incorrect because the ISP is a company that provides access to the Internet and related services to the organization. The ISP does not define the organization??s policies and rules, but may have its own policies and rules that the organization has to comply with as a customer4. Option D, the cloud provider, is incorrect because the cloud provider is a company that provides cloud computing services to the organization. The cloud provider does not define the organization??s policies and rules, but may have its own policies and rules that the organization has to comply with as a
customer5. References :=
? Policy Violation Definition | Law Insider1
? How to Write Policies and Procedures | Smartsheet2
? What is an External Auditor? - Definition from Safeopedia3
? What is an Internet Service Provider (ISP)? - Definition from Techopedia4
? What is Cloud Provider? - Definition from Techopedia

NEW QUESTION 161
Which of the following is a cloud-specific security standard?

A. 15027017
B. 15014001
C. 15022301
D. 15027701

Answer: A

Explanation:
ISO/IEC 15027017 is a cloud-specific security standard that provides guidelines for information security controls applicable to the provision and use of cloud services. It is based on ISO/IEC 27002, which is a general standard for information security management, but it also includes additional controls and implementation guidance that specifically relate to cloud services. ISO/IEC 15027017 is intended to help both cloud service providers and cloud service customers to enhance the security and confidentiality of their cloud environment and to comply with relevant regulatory requirements and industry standards.12 References := ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services1; Cloud Security Standards: ISO, PCI, GDPR and Your Cloud - Exabeam3; ISO/IEC 27017 - Wikipedia2

NEW QUESTION 166
Who is accountable for the use of a cloud service?

A. The cloud access security broker (CASB)
B. The supplier
C. The cloud service provider
D. The organization (client)

Answer: D

Explanation:
The organization (client) is accountable for the use of a cloud service. Accountability in cloud computing is the responsibility of cloud service providers and other parties in the cloud ecosystem to protect and properly process the data of their clients and users. However, accountability ultimately rests with the organization (client) that uses the cloud service, as it is the data owner and controller. The organization (client) has to ensure that the cloud service provider and its suppliers meet the agreed-upon service levels, security standards, and regulatory requirements. The organization (client) also has to perform due diligence and oversight on the cloud service provider and its suppliers, as well as to comply with the shared responsibility model, which defines how the security and compliance tasks and obligations are divided between the cloud service provider and the organization (client)123.
The other options are not correct. Option A, the cloud access security broker (CASB), is incorrect because a CASB is a software tool or service that acts as an intermediary between cloud users and cloud service providers, providing visibility, data security, threat protection, and compliance. A CASB does not use the cloud service, but facilitates its secure and compliant use4. Option B, the supplier, is incorrect because a supplier is a third-party entity that provides services or products to the cloud service provider, such as infrastructure, software, hardware, or support. A supplier does not use the cloud service, but supports its delivery5. Option C, the cloud service provider, is incorrect because a cloud service provider is a company that provides cloud computing services to the organization (client). A cloud service provider does not use the cloud service, but offers it to the organization (client)6. References :=
? Accountability Issues in Cloud Computing (5 Step ?? - Medium1
? Shared responsibility in the \uE000cloud\uE001 - Microsoft Azure2
? Who Is Responsible for Cloud Security? - Security Intelligence3
? What is CASB? - Cloud Security Alliance4
? Cloud Computing: Auditing Challenges - ISACA5
? What is Cloud Provider? - Definition from Techopedia

NEW QUESTION 171
An auditor is auditing the services provided by a cloud service provider. When evaluating the security of the cloud customer's data in the cloud, which of the following should be of GREATEST concern to the auditor?

A. Personally identifiable information (Pll) is pseudonymized but not fully encrypted.
B. The cloud customer has encrypted the confidential data in the cloud using its own encryption keys.
C. The confidential data stored in the cloud is encrypted using encryption keys that are managed by the provider.
D. According to the cloud customer's data handling policy, all confidential data should be encrypted, but the confidential data stored in the cloud is well segmented

but not encrypted.

Answer: A

NEW QUESTION 175
To support a customer's verification of the cloud service provider claims regarding its responsibilities according to the shared responsibility model, which of the following tools and techniques is appropriate?

A. External audit
B. Internal audit
C. Contractual agreement
D. Security assessment

Answer: C

Explanation:
An external audit is an appropriate tool and technique to support a customer??s verification of the cloud service provider??s claims regarding its responsibilities according to the shared responsibility model. An external audit is an independent and objective examination of the cloud service provider??s policies, procedures, controls, and performance by a qualified third-party auditor. An external audit can provide assurance that the cloud service provider is fulfilling its obligations and meeting the customer??s expectations in terms of security, compliance, availability, reliability, and quality. An external audit can also identify any gaps or weaknesses in the cloud service provider??s security posture and suggest recommendations for improvement.
An external audit can be based on various standards, frameworks, and regulations that are relevant to the cloud service provider??s industry and domain. For example, some common external audits for cloud service providers are:
? ISO/IEC 27001: This is an international standard that specifies the requirements
for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive information so that it remains secure. An ISO/IEC 27001 certification demonstrates that the cloud service provider has implemented
a comprehensive and effective ISMS that covers all aspects of information security, including risk assessment, policy development, asset management,
access control, incident management, business continuity, and compliance.1
? SOC 2: This is an attestation report that evaluates the cloud service provider??s security controls based on the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria. The Trust Services Criteria are a set of principles and criteria for evaluating the design and operating effectiveness of controls that affect the security, availability, processing integrity, confidentiality, and privacy of a system. A SOC 2 report provides assurance that the cloud service provider has implemented adequate controls to protect the customer??s data and systems.2
? CSA STAR: This 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 CSA STAR program consists of three levels of assurance: Level 1: Self-Assessment, Level 2: Third-Party Audit, and Level 3: Continuous Auditing. The CSA STAR program aims to provide transparency, assurance, and trust in the cloud ecosystem by enabling customers to assess and compare the security and compliance posture of cloud service providers.3
The other options listed are not suitable for supporting a customer??s verification of the cloud service provider??s claims regarding its responsibilities according to the shared responsibility model. An internal audit is an audit conducted by the cloud service provider itself or by an internal auditor hired by the cloud service provider. An internal audit may not be as independent or objective as an external audit, and it may not provide sufficient evidence or credibility to the customer. A contractual agreement is a legal document that defines the roles, responsibilities, expectations, and obligations of both the cloud service provider and the customer. A contractual agreement may specify the terms and conditions for service delivery, performance, availability, security, compliance, data protection, incident response, dispute resolution, liability, and termination. However, a contractual agreement alone does not verify or validate whether the cloud service provider is actually fulfilling its claims or meeting its contractual obligations. A security assessment is a process of identifying, analyzing, and evaluating the security risks and vulnerabilities of a system or an organization. A security assessment may involve various methods such as vulnerability scanning, penetration testing, threat modeling, or risk analysis. A security assessment may provide useful information about the current state of security of a system or an organization, but it may not cover all aspects of the shared responsibility model or provide assurance that the cloud service provider is complying with its responsibilities on an ongoing basis.

NEW QUESTION 177
The CSA STAR Certification is based on criteria outlined the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) in addition to:

A. GDPR CoC certification.
B. GB/T 22080-2008.
C. SOC 2 Type 1 or 2 reports.
D. ISO/IEC 27001 implementation.

Answer: D

Explanation:
The CSA STAR Certification is based on criteria outlined in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) in addition to ISO/IEC 27001 implementation. The CCM is a cybersecurity control framework for cloud computing that covers 17 domains and 197 control objectives that address all key aspects of cloud technology. ISO/IEC 27001 is a standard for information security management systems that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. The CSA STAR Certification demonstrates that a cloud service provider conforms to the applicable requirements of ISO/IEC 27001, has addressed issues critical to cloud security as outlined in the CCM, and has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas1. The CSA STAR Certification is a third-party independent assessment of the security of a cloud service provider and provides a high level of assurance and trust to customers2.
References:
? CSA STAR Certification - Azure Compliance | Microsoft Learn
? STAR | CSA

NEW QUESTION 182
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?

A. 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.
B. Validate whether the strategy is developed by both cloud service providers and cloud service consumers within the acceptable limits of their risk appetite.
C. 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.

Answer: A

NEW QUESTION 187
Which of the following would be considered as a factor to trust in a cloud service provider?

A. The level of willingness to cooperate
B. The level of exposure for public information
C. The level of open source evidence available
D. The level of proven technical skills

Answer: C

Explanation:
Trust in a cloud service provider is fundamentally based on the assurance that the provider can deliver secure and reliable services. The level of proven technical skills is a critical factor because it demonstrates the provider??s capability to implement and maintain robust security measures, manage complex cloud infrastructures, and respond effectively to technical challenges. Technical expertise is essential for establishing trust, as it directly impacts the security and performance of the cloud services offered.
References = The importance of technical skills in establishing trust is supported by the resources provided by ISACA and the Cloud Security Alliance (CSA). These resources emphasize the need for cloud service providers to have a strong technical foundation to ensure the fulfillment of internal requirements, proper controls, and compliance with regulations, which are crucial for maintaining customer trust and mitigating risks1234.

NEW QUESTION 189
When applying the Top Threats Analysis methodology following an incident, what is the scope of the technical impact identification step?

A. Determine the impact on the controls that were selected by the organization to respond toidentified risks.
B. Determine the impact on confidentiality, integrity, and availability of the information system.
C. Determine the impact on the physical and environmental security of the organization, excluding informational assets.
D. Determine the impact on the financial, operational, compliance, and reputation of the organization.

Answer: B

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

NEW QUESTION 194
When performing audits in relation to the organizational strategy and governance, what should be requested from the cloud service provider?

A. Enterprise cloud security strategy
B. Enterprise cloud strategy and policy
C. Attestation reports
D. Policies and procedures

Answer: C

NEW QUESTION 198
Which of the following activities is performed outside information security monitoring?

A. Management review of the information security framework
B. Monitoring the effectiveness of implemented controls
C. Collection and review of security events before escalation
D. Periodic review of risks, vulnerabilities, likelihoods, and threats

Answer: A

Explanation:
The management review of the information security framework is an activity that typically occurs outside the regular scope of information security monitoring. This review is a strategic exercise that involves evaluating the overall direction, effectiveness, and alignment of the information security program with the organization??s objectives and risk appetite. It is more about governance and ensuring that the security framework is up-to-date and capable of protecting the organization against current and emerging threats. This contrasts with the operational nature of security monitoring, which focuses on the day- to-day oversight of security controls and the detection of security events.
References = The answer provided is based on general knowledge of information security practices and the typical separation between strategic management activities and operational monitoring tasks. Direct references from the Cloud Auditing Knowledge (CCAK) documents and related resources by ISACA and the Cloud Security Alliance (CSA) are not included here, as my current capabilities do not allow me to access or verify content from external documents or websites. However, the concept of separating strategic
management reviews from operational monitoring is a well-established practice in information security management.

NEW QUESTION 203
What is below the waterline in the context of cloud operationalization?

A. The controls operated by the customer
B. The controls operated by both
C. The controls operated by the cloud access security broker (CASB)
D. The controls operated by the cloud service provider

Answer: D

Explanation:
In the context of cloud operationalization, ??below the waterline?? refers to the aspects of cloud services that are managed and controlled by the cloud service provider (CSP) rather than the customer. This analogy is often used to describe the shared responsibility model in cloud computing, where the CSP is responsible for the infrastructure??s security and stability, akin to the submerged part of an iceberg that supports the structure above water. The customer, on the other hand, is responsible for managing the controls and security measures ??above the waterline,?? which include the applications, data, and access management they deploy in the cloud environment.
References = The information provided is based on standard cloud computing models and the shared responsibility concept, which is a fundamental principle discussed in cloud auditing and security literature, including the CCAK curriculum and related resources1.

NEW QUESTION 207
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?

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 offerings1 The 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 to1 The 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)2 The 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 trustworthiness1 The 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.
References: 1: STAR | CSA 2: Why your cloud services need the CSA STAR Registry listing 3: STAR Registry | CSA

NEW QUESTION 212
What is the FIRST thing to define when an organization is moving to the cloud?

A. Goals of the migration
B. Internal service level agreements (SLAs)
C. Specific requirements
D. Provider evaluation criteria

Answer: A

Explanation:
When an organization is moving to the cloud, the first thing to define is the goals of the migration. This is because the goals will guide all subsequent decisions and strategies. Defining clear goals helps in understanding what the organization wants to achieve with cloud migration, whether it??s cost savings, scalability, improved performance, or something else. These goals are essential for aligning the migration with the business objectives and for setting the direction for the cloud strategy.
References = The importance of defining the goals of cloud migration is supported by the resources provided by the Cloud Security Alliance (CSA) and ISACA in their Cloud Auditing Knowledge (CCAK) materials12. These resources emphasize the need for a clear understanding of the objectives and benefits expected from moving to the cloud, which is foundational before delving into specifics such as SLAs, requirements, or provider evaluation criteria.

NEW QUESTION 214
......