Exam Questions CCAK

Certificate of Cloud Auditing Knowledge

https://www.2passeasy.com/dumps/CCAK/

NEW QUESTION 1
Supply chain agreements between a cloud service provider and cloud customers should, at a minimum, include:

A. regulatory guidelines impacting the cloud customer.
B. audits, assessments, and independent verification of compliance certifications with agreement terms.
C. policies and procedures of the cloud customer
D. the organizational chart of the provider.

Answer: B

Explanation:
Supply chain agreements between a cloud service provider and cloud customers should, at a minimum, include audits, assessments, and independent verification of compliance certifications with agreement terms. This is because cloud customers need to ensure that the cloud service provider meets the agreed-upon service levels, security standards, and regulatory requirements. Audits, assessments, and independent verification can provide evidence of the cloud service provider??s compliance
and performance and help identify any gaps or risks that need to be addressed. This is also stated in the Practical Guide to Cloud Service Agreements Version 2.012, which is a reference document for cloud customers and providers to analyze and negotiate cloud service agreements.
The other options are not directly related to the question. Option A, regulatory guidelines impacting the cloud customer, refers to the legal and ethical obligations that the cloud customer has to comply with when using cloud services, such as data protection, privacy, and security laws. These guidelines may vary depending on the jurisdiction, industry, and type of data involved. Option C, policies and procedures of the cloud customer, refers to the internal rules and processes that the cloud customer has to follow when using cloud services, such as data governance, access management, and incident response. Option D, the organizational chart of the provider, refers to the structure and hierarchy of the cloud service provider??s organization, such as the roles, responsibilities, and relationships of its employees, departments, and units.
References :=
? Practical Guide to Cloud Service Agreements Version 2.01
? Practical Guide to Cloud Service Agreements V2.0| Object ?? - OMG3
? Supply chain agreements between CSP and cloud customers should ??4
? Practical Guide to Cloud Service Agreements Version 3

NEW QUESTION 2
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 3
What areas should be reviewed when auditing a public cloud?

A. Identity and access management (IAM) and data protection
B. Source code reviews and hypervisor
C. Patching and configuration
D. Vulnerability management and cyber security reviews

Answer: A

Explanation:
When auditing a public cloud, it is essential to review areas such as Identity and Access Management (IAM) anddata protection. IAM involves ensuring that only authorized individuals have access to the cloud resources, and that their access is appropriately managed and monitored. This includes reviewing user authentication methods, access control policies, role-based access controls, and user activity monitoring1. Data protection is another critical area to review. It involves ensuring that the data stored in the public cloud is secure from unauthorized access, breaches, and leaks. This includes reviewing data encryption methods, data backup and recovery processes, data privacy policies, and compliance with relevant data protection regulations1.
While the other options may also be relevant in certain contexts, they are not as universally
applicable as IAM and data protection for auditing a public cloud. Source code reviews and hypervisor (option B), patching and configuration (option C), and vulnerability management and cybersecurity reviews (option D) are important but are more specific to certain types of cloud services or deployment models.
References:
? Cloud Computing — What IT Auditors Should Really Know - ISACA

NEW QUESTION 4
Under GDPR, an organization should report a data breach within what time frame?

A. 48 hours
B. 72 hours
C. 1 week
D. 2 weeks

Answer: B

Explanation:
Under the General Data Protection Regulation (GDPR), organizations are required to report a data breach to the appropriate supervisory authority within 72 hours of becoming aware of it. This timeframe is critical to ensure timely communication with the authorities and affected individuals, if necessary, to mitigate any potential harm caused by the breach.
References = This requirement is outlined in the GDPR guidelines, which emphasize the importance of prompt reporting to maintain compliance and protect individual rights and freedoms12345.

NEW QUESTION 5
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 6
Which of the following is a KEY benefit of using the Cloud Controls Matrix (CCM)?

A. CCM utilizes an ITIL framework to define the capabilities needed to manage the IT services and security services.
B. CCM maps to existing security standards, best practices, and regulations.
C. CCM uses a specific control for Infrastructure as a Service (IaaS).
D. CCM V4 is an improved version from CCM V3.0.1.

Answer: B

Explanation:
The Cloud Controls Matrix (CCM) is a cybersecurity control framework specifically designed for cloud computing environments. A key benefit of using the CCM is that it maps to existing security standards, best practices, and regulations. This mapping allows organizations to ensure that their cloud security posture aligns with industry- recognized frameworks, thereby facilitating compliance and security assurance efforts. The CCM??s comprehensive set of control objectives covers all key aspects of cloud technology and provides guidance on which security controls should be implemented by various actors within the cloud supply chain.
References = This answer is supported by the information provided in the Cloud Controls Matrix documentation and related resources, which highlight the CCM??s alignment with other security standards and its role in helping organizations navigate the complex landscape of cloud security and compliance12.

NEW QUESTION 7
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 8
A cloud auditor observed that just before a new software went live, the librarian transferred production data to the test environment to confirm the new software can work in the production environment. What additional control should the cloud auditor check?

A. Approval of the change by the change advisory board
B. Explicit documented approval from all customers whose data is affected
C. Training for the librarian
D. Verification that the hardware of the test and production environments are compatible

Answer: B

Explanation:
The cloud auditor should check if there is explicit documented approval from all customers whose data is affected by the transfer of production data to the test environment. This is because production data may contain sensitive or personal
information that is subject to privacy and security regulations, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA). Therefore, using production data for testing purposes without the consent of the data owners may violate their rights and expose the organization to legal and reputational risks. This is also stated in the Cloud Controls Matrix (CCM) control DSI-04: Production / Non-Production Environments12, which is part of the Data Security & Information Lifecycle Management domain. The 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 other options are not directly related to the question. Option A, approval of the change by the change advisory board, refers to the process of reviewing and authorizing changes
to the system or software before they are implemented in the production environment. This is a good practice for ensuring the quality and reliability of the system or software, but it does not address the issue of using production data for testing purposes. Option C, training for the librarian, refers to the process of providing adequate education and awareness to the staff who are responsible for managing and transferring data between different environments. This is a good practice for ensuring the competence and accountability of the staff, but it does not address the issue of obtaining consent from the data owners. Option D, verification that the hardware of the test and production environments are compatible, refers to the process of ensuring that the system or software can run smoothly and consistently on both environments. This is a good practice for ensuring the performance and functionality of the system or software, but it does not address the issue of protecting the privacy and security of the production data. References :=
? Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, Chapter 6: Cloud
Security Controls
? Cloud Controls Matrix (CCM) - CSA3
? DSI-04: Production / Non-Production Environments - CSF Tools - Identity Digital1
? DSI: Data Security & Information Lifecycle Management - CSF Tools - Identity Digital

NEW QUESTION 9
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 10
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
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 12
A dot release of the Cloud Controls Matrix (CCM) indicates:

A. a revision of the CCM domain structure.
B. a technical change (revision, addition, or deletion) of a number of controls that is smaller than 10% compared to the previous full release.
C. the introduction of new control frameworks mapped to previously published CCM controls.
D. technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release.

Answer: B

Explanation:
A dot release of the Cloud Controls Matrix (CCM) indicates a technical change (revision, addition, or deletion) of a number of controls that is smaller than 10% compared to the previous full release. A dot release is a minor update to the CCM that reflects the feedback from the cloud security community and the changes in the cloud technology landscape. A dot release does not change the domain structure or the overall scope of the CCM, but rather improves the clarity, accuracy, and relevance of the existing controls. A dot release is denoted by a decimal number after the major version number, such as CCM v4.1 or CCM v4.2. The current version of the CCM is v4.0, which was released in October 20211.
The other options are incorrect because:
? A. a revision of the CCM domain structure: A revision of the CCM domain structure is a major change that affects the organization and categorization of the controls into different domains. A revision of the CCM domain structure requires a full release, not a dot release, and is denoted by an integer number, such as CCM v3 or CCM v42.
? C. the introduction of new control frameworks mapped to previously published CCM controls: The introduction of new control frameworks mapped to previously published CCM controls is an additional feature that enhances the usability and
applicability of the CCM. The introduction of new control frameworks mapped to previously published CCM controls does not require a dot release or a full release, but rather an update to the mapping table that shows the relationship between the CCM controls and other industry-accepted security standards, regulations, and frameworks3.
? D. technical change (revision, addition, or deletion) of a number of controls that is
greater than 10% compared to the previous full release: A technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release is a significant change that affects the content and scope of the CCM. A technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release requires a full release, not a dot release, and is denoted by an integer number, such as CCM v3 or CCM v42.
References:
? Cloud Controls Matrix (CCM) - CSA
? The CSA Cloud Controls Matrix (CCM) V4: Raising the cloud security bar
? Cloud Security Alliance Releases New Cloud Controls Matrix Auditing Guidelines

NEW QUESTION 16
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 18
In all three cloud deployment models, (laaS, PaaS, and SaaS), who is responsible for the patching of the hypervisor layer?

A. Cloud service provider
B. Shared responsibility
C. Cloud service customer

D. Patching on hypervisor layer not required

Answer: A

Explanation:
The cloud service provider is responsible for the patching of the hypervisor layer in all three cloud deployment models (IaaS, PaaS, and SaaS). The hypervisor layer is the software that allows the creation and management of virtual machines on a physical server. The hypervisor layer is part of the cloud infrastructure, which is owned and operated by the cloud service provider. The cloud service provider is responsible for ensuring that the hypervisor layer is secure, reliable, and up to date with the latest patches and updates. The cloud service provider should also monitor and report on the status and performance of the hypervisor layer, as well as any issues or incidents that may affect it. The cloud service customer is not responsible for the patching of the hypervisor layer, as they do not have access or control over the cloud infrastructure. The cloud service customer only has access and control over the cloud resources and services that they consume from the cloud service provider, such as virtual machines, storage, databases, applications, etc. The cloud service customer is responsible for ensuring that their own cloud resources and services are secure, compliant, and updated with the latest patches and updates.
The patching of the hypervisor layer is not a shared responsibility between the cloud service provider and the cloud service customer, as it is solely under the domain of the cloud service provider. The shared responsibility model in cloud computing refers to the division of security and compliance responsibilities between the cloud service provider and the cloud service customer, depending on the type of cloud deployment model. For example, in IaaS, the cloud service provider is responsible for securing the physical infrastructure, network, and hypervisor layer, while the cloud service customer is responsible for securing their own operating systems, applications, data, etc. In PaaS, the cloud service provider is responsible for securing everything up to the platform layer, while the cloud service customer is responsible for securing their own applications and data. In SaaS, the cloud service provider is responsible for securing everything up to the application layer, while the cloud service customer is responsible for securing their own data and user access.
Patching on hypervisor layer is required, as it is essential for maintaining the security, reliability, and performance of the cloud infrastructure. Patching on hypervisor layer can help prevent vulnerabilities, bugs, errors, or exploits that may compromise or affect the functionality of the virtual machines or other cloud resources and services. Patching on hypervisor layer can also help improve or enhance the features or capabilities of the hypervisor software or hardware.
References :=
? Patching process - AWS Prescriptive Guidance
? What is a Hypervisor in Cloud Computing and Its Types? - Simplilearn
? In all three cloud deployment models, (IaaS, PaaS, and ?? - Exam4Training
? Reference Architecture: App Layering | Citrix Tech Zone
? Hypervisor - GeeksforGeeks

NEW QUESTION 23
Which of the following should a cloud auditor recommend regarding controls for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse?

A. Assessment of contractual and regulatory requirements for customer access
B. Establishment of policies and procedures across multiple system interfaces, jurisdictions,and business functions to prevent improper disclosure, alteration, or destruction
C. Data input and output integrity routines
D. Testing in accordance with leading industry standards such as OWASP

Answer: C

Explanation:
The correct answer is C. Data input and output integrity routines (i.e., reconciliation and edit checks) are controls that can be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse. This is stated in the Cloud Controls Matrix (CCM) control AIS-03: Data Integrity123, which is part of the Application & Interface Security domain. The 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 other options are not directly related to the question. Option A refers to the CCM control AIS-02: Customer Access Requirements2, which addresses the security, contractual, and regulatory requirements for customer access to data, assets, and information systems. Option B refers to the CCM control AIS-04: Data Security / Integrity2, which establishes policies and procedures to support data security across multiple system
interfaces, jurisdictions, and business functions. Option D refers to the CCM control AIS-01: Application Security2, which requires applications and programming interfaces (APIs) to be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications). References :=
? Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, Chapter 5: Cloud Assurance Frameworks
? What is the Cloud Controls Matrix (CCM)? - Cloud Security Alliance4
? AIS-03: Data Integrity - CSF Tools - Identity Digital1
? AIS: Application & Interface Security - CSF Tools - Identity Digital2
? PR.DS-6: Integrity checking mechanisms are used to verify software ?? - CSF Tools - Identity Digital

NEW QUESTION 24
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 26
Which of the following is a tool that visually depicts the gaps in an organization's security capabilities?

A. Cloud security alliance (CSA) cloud control matrix
B. Requirements traceability matrix
C. Cloud security alliance (CSA) enterprise architecture (EA)
D. Colored impact and likelihood risk matrix

Answer: C

NEW QUESTION 29
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 32
The BEST way to deliver continuous compliance in a cloud environment is to:

A. combine point-in-time assurance approaches with continuous monitoring.
B. increase the frequency of external audits from annual to quarterly.
C. combine point-in-time assurance approaches with continuous auditing.
D. decrease the interval between attestations of compliance

Answer: A

Explanation:
Continuous auditing is a method of auditing that provides assurance on the current state of controls and compliance in a cloud environment, rather than relying on periodic snapshots or attestations. Continuous auditing can leverage continuous monitoring data and automated tools to collect and analyze evidence of compliance, as well as alert auditors and stakeholders of any deviations or issues. Continuous auditing can complement point-in-time assurance approaches, such as certifications or audits, by providing more timely and frequent feedback on the effectiveness of controls and compliance in a cloud environment. References :=
? ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021,p. 821
? ISACA, Cloud Auditing Knowledge: Preparing for the CCAK Certificate Exam, 2021, p. 30

NEW QUESTION 34
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 35
Which of the following is the PRIMARY component to determine the success or failure of an organization??s cloud compliance program?

A. Defining the metrics and indicators to monitor the implementation of the compliance program
B. Determining the risk treatment options to be used in the compliance program
C. Mapping who possesses the information and data that should drive the compliance goals
D. Selecting the external frameworks that will be used as reference

Answer: C

Explanation:
The primary component to determine the success or failure of an organization??s cloud compliance program is mapping who possesses the information and data that should drive the compliance goals. This is because the cloud compliance program should be aligned with the organization??s business objectives and risk appetite, and the information and data that support these objectives and risks are often distributed across different cloud service providers, business units, and stakeholders. Therefore, it is essential to identify who owns, controls, and accesses the information and data, and how they are protected, processed, and shared in the cloud environment. This is part of the Cloud Control Matrix (CCM) domain COM-02: Data Governance, which states that "The organization should have a policy and procedures to manage data throughout its lifecycle in accordance with regulatory requirements, contractual obligations, and industry standards."1
References := CCAK Study Guide, Chapter 3: Cloud Compliance Program, page 53

NEW QUESTION 39
In a situation where duties related to cloud risk management and control are split between an organization and its cloud service providers, which of the following would BEST help to ensure a coordinated approach to risk and control processes?

A. Establishing a joint security operations center
B. Automating reporting of risk and control compliance
C. Co-locating compliance management specialists
D. Maintaining a centralized risk and controls dashboard

Answer: D

Explanation:
A centralized risk and controls dashboard is the best option for ensuring a coordinated approach to risk and control processes when duties are split between an organization and its cloud service providers. This dashboard provides a unified view of risk and control status across the organization and the cloud services it utilizes. It enables both parties to monitor and manage risks effectively and ensures that control activities are aligned and consistent. This approach supports proactive risk management and facilitates communication and collaboration between the organization and the cloud service provider. References = The concept of a centralized risk and controls dashboard is supported by the Cloud Security Alliance (CSA) and ISACA, which emphasize the importance of visibility and coordination in cloud risk management. The CCAK materials and the Cloud Controls Matrix (CCM) provide guidance on establishing such dashboards as a means to manage and mitigate risks in a cloud environment12.

NEW QUESTION 42
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 45
Which of the following is the BEST method to demonstrate assurance in the cloud services to multiple cloud customers?

A. Provider??s financial stability report and market value
B. Reputation of the service provider in the industry
C. Provider self-assessment and technical documents
D. External attestation and certification audit reports

Answer: D

Explanation:
External attestation and certification audit reports are considered the best method to demonstrate assurance in cloud services to multiple customers because they provide an independent verification of the cloud service provider??s controls and practices. These reports are conducted by third-party auditors and offer a level of transparency and trust that cannot be achieved through self-assessments or internal documents. They help ensure that the cloud provider meets industry standards and regulatory requirements, which is crucial for customers to assess the risk and compliance posture of their cloud service providers.
References = The importance of external attestation and certification audit reports is supported by the Cloud Security Alliance (CSA) and ISACA, which state that the CCAK credential prepares IT and security professionals to ensure that the right controls are in place and to mitigate the risks and costs of audit management and penalties for non- compliance1.

NEW QUESTION 48
What does ??The Egregious 11" refer to?

A. The OWASP Top 10 adapted to cloud computing
B. A list of top shortcomings of cloud computing
C. A list of top breaches in cloud computing
D. A list of top threats to cloud computing

Answer: D

Explanation:
The Egregious 11 refers to a list of top threats to cloud computing, as published by the Cloud Security Alliance (CSA) in 2019. The CSA is a leading organization dedicated to defining standards, certifications and best practices to help ensure a secure cloud computing environment. The Egregious 11 report ranks the most critical and pressing cloud security issues, such as data breaches, misconfigurations, insufficient identity and access management, and account hijacking. The report also provides recommendations for security, compliance, risk and technology practitioners to mitigate these threats. The Egregious 11 is based on a survey of industry experts and a review of current literature and media reports. The report is intended to raise awareness of the risks and challenges associated with cloud computing and promote strong security practices.12 References := CCAK Study Guide, Chapter 5: Cloud Auditing, page 961; CSA Top Threats to Cloud Computing: Egregious 11

NEW QUESTION 51
What is a sign that an organization has adopted a shift-left concept of code release cycles?

A. Large entities with slower release cadences and geographically dispersed systems
B. A waterfall model to move resources through the development to release phases
C. Maturity of start-up entities with high-iteration to low-volume code commits
D. Incorporation of automation to identify and address software code problems early

Answer: D

Explanation:
The shift-left concept of code release cycles is an approach that moves testing, quality, and performance evaluation early in the development process, often before any code is written. The goal of shift-left testing is to anticipate and resolve software defects, bugs, errors, and vulnerabilities as soon as possible, reducing the cost and time of fixing them later in the production stage. To achieve this, shift-left testing relies on automation tools and techniques that enable continuous integration, continuous delivery, and continuous deployment of code. Automation also facilitates collaboration and feedback among developers, testers, security experts, and other stakeholders throughout the
development lifecycle. Therefore, the incorporation of automation to identify and address software code problems early is a sign that an organization has adopted a shift-left concept of code release cycles. References:
? The ??Shift Left?? Is A Growing Theme For Cloud Cybersecurity In 2022
? Shift left vs shift right: A DevOps mystery solved
? How to shift left with continuous integration

NEW QUESTION 55
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 59
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 62
For an auditor auditing an organization's cloud resources, which of the following should be of GREATEST concern?

A. The organization does not have separate policies for governing its cloud environment.
B. The organization's IT team does not include resources with cloud certifications.
C. The organization does not perform periodic reviews or control monitoring for its cloud environment, but it has a documented audit plan and performs an audit for its cloud environment every alternate year.
D. The risk management team reports to the head of audit.

Answer: C

NEW QUESTION 64
Visibility to which of the following would give an auditor the BEST view of design and implementation decisions when an organization uses programmatic automation for Infrastructure as a Service (IaaS) deployments?
A. Source code within build scripts
B. Output from threat modeling exercises
C. Service level agreements (SLAs)
D. Results from automated testing

Answer: A

Explanation:
Visibility to the source code within build scripts would give an auditor the best view of design and implementation decisions when an organization uses programmatic automation for Infrastructure as a Service (IaaS) deployments. IaaS is a cloud service model that provides virtualized computing resources, such as servers, storage, network, and operating systems, over the internet. Programmatic automation is the process of using code or scripts to automate the provisioning, configuration, management, and monitoring of the cloud infrastructure. Build scripts are files that contain commands or instructions to create or modify the cloud infrastructure according to the desired specifications.12
An auditor can use the source code within build scripts to gain insight into how the organization designs and implements its cloud infrastructure. The source code can reveal the following information3:
? The type, size, and number of cloud resources that are provisioned and deployed
? The configuration settings and parameters that are applied to the cloud resources
? The security controls and policies that are enforced on the cloud resources
? The dependencies and relationships between the cloud resources
? The testing and validation methods that are used to verify the functionality and performance of the cloud resources
? The logging and auditing mechanisms that are used to track and record the changes and activities on the cloud resources
By reviewing the source code within build scripts, an auditor can evaluate whether the organization follows the best practices and standards for cloud infrastructure design and implementation, such as scalability, reliability, security, compliance, and efficiency. An auditor can also identify any gaps or risks in the organization??s cloud infrastructure and provide recommendations for improvement.
References := What is Infrastructure as Code? | Cloud Computing - AWS1; What is Programmatic Automation? - Definition from Techopedia2; How to audit your IaC for better DevSecOps - TechBeacon3

NEW QUESTION 67
The MOST important factor to consider when implementing cloud-related controls is the:
A. shared responsibility model.
B. effectiveness of the controls.
C. risk reporting.
D. risk ownership

Answer: A

Explanation:
The most important factor to consider when implementing cloud-related controls is the shared responsibility model. The shared responsibility model is a framework that defines the roles and responsibilities of cloud service providers (CSPs) and cloud customers (CCs) in ensuring the security and compliance of cloud computing environments. The shared responsibility model helps to clarify which security tasks are handled by the CSP and which tasks are handled by the CC, depending on the type of cloud service model (IaaS, PaaS, SaaS) and the specific contractual agreements. The shared responsibility model also helps to avoid gaps or overlaps in security controls, and to allocate resources and accountability accordingly12.
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
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 73
From a compliance perspective, which of the following artifacts should an assessor review when evaluating the effectiveness of Infrastructure as Code deployments?

A. Evaluation summaries
B. logs
C. SOC reports
D. Interviews

Answer: B

Explanation:
From a compliance perspective, reviewing logs is crucial when evaluating the effectiveness of Infrastructure as Code (IaC) deployments. Logs provide a detailed record of events, changes, and operations that have occurred within the IaC environment. They are essential for tracking the deployment process, identifying issues, and verifying that the infrastructure has been configured and is operating as intended. Logs can also be used to ensure that the IaC deployments comply with security policies and regulatory requirements, making them a vital artifact for assessors.
References = The importance of logs in assessing IaC deployments is supported by cybersecurity best practices, which recommend the use of logs for auditable records of changes to template files and for tracking resource protection1. Additionally, ISACA??s resources on securing IaC highlight the role of logs in providing transparency and enabling infrastructure blueprints to be audited and reviewed for common errors or misconfigurations2.

NEW QUESTION 76
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 78
To qualify for CSA STAR attestation for a particular cloud system, the SOC 2 report must cover:

A. Cloud Controls Matrix (CCM) and ISO/IEC 27001:2013 controls.
B. ISO/IEC 27001:2013 controls.
C. all Cloud Controls Matrix (CCM) controls and TSPC security principles.
D. maturity model criteria.

Answer: A

Explanation:
To qualify for CSA STAR attestation, the SOC 2 report must cover both the Cloud Controls Matrix (CCM) and ISO/IEC 27001:2013 controls. The CSA STAR Attestation integrates SOC 2 reporting with additional cloud security criteria from the CSA CCM. This combination provides a comprehensive framework for assessing the security and privacy controls of cloud services, ensuring that they meet the rigorous standards required for STAR attestation. References = The information is supported by the Cloud Security Alliance??s resources, which outline the STAR program??s emphasis on transparency, rigorous auditing, and harmonization of standards as per the CCM. Additionally, the CSA STAR Certification process leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix

NEW QUESTION 79
Which of the following approaches encompasses social engineering of staff, bypassing of physical access controls, and penetration testing?

A. Red team
B. Blue team
C. White box
D. Gray box

Answer: A

Explanation:
The approach that encompasses social engineering of staff, bypassing of physical access controls, and penetration testing is typically associated with a Red team. A Red team is designed to simulate real-world attacks to test the effectiveness of security measures. They often use tactics like social engineering and penetration testing to identify vulnerabilities. In contrast, a Blue team is responsible for defending against attacks, a White box approach involves testing with internal knowledge of the system, and a Gray box is a combination of both White box and Black box testing methods.
References = The information aligns with the principles of cloud auditing and security assessments as outlined in the resources provided by ISACA and the Cloud Security Alliance, which emphasize the importance of understanding various security testing methodologies to effectively audit cloud systems123.

NEW QUESTION 83
An independent contractor is assessing the security maturity of a Software as a Service (SaaS) company against industry standards. The SaaS company has developed and hosted all its products using the cloud services provided by a third-party cloud service provider. What is the optimal and most efficient mechanism to assess the controls provider is responsible for?

A. Review the provider's published questionnaires.
B. Review third-party audit reports.
C. Directly audit the provider.
D. Send a supplier questionnaire to the provider.

Answer: B

Explanation:
The optimal and most efficient mechanism to assess the controls that the provider is responsible for is to review third-party audit reports. Third-party audit reports are independent and objective assessments of the provider??s security, compliance, and performance, conducted by qualified and reputable auditors. Third-party audit reports can provide assurance and evidence that the provider meets the industry standards and best practices, as well as the contractual and legal obligations with the SaaS company. Third- party audit reports can also cover a wide range of controls, such as data security, encryption, identity and access management, incident response, disaster recovery, and service level agreements. Some examples of third-party audit reports are ISO 27001 certification, SOC 1/2/3 reports, CSA STAR certification, and FedRAMP authorization123. Reviewing the provider??s published questionnaires (A) may not be optimal or efficient, as the published questionnaires may not be comprehensive or up-to-date, and may not reflect the actual state of the provider??s controls. The published questionnaires may also be biased or inaccurate, as they are produced by the provider themselves.
Directly auditing the provider © may not be feasible or necessary, as the independent contractor may not have access to the provider??s environment or data, and may not have the authority or expertise to conduct such an audit. The independent contractor should rely on the third-party audit reports and certifications to assess the provider??s compliance with relevant standards and regulations.
Sending a supplier questionnaire to the provider (D) may not be optimal or efficient, as the supplier questionnaire may not cover all the aspects of the provider??s controls, and may not provide sufficient evidence or assurance of the provider??s security maturity. The supplier questionnaire may also take a long time to complete and verify, and may not be consistent with the industry standards and best practices. References :=
? How to Evaluate Cloud Service Provider Security (Checklist)
? Cloud service review process - Cloud Adoption Framework

? How to choose a cloud service provider | Microsoft Azure

NEW QUESTION 84
is it important for the individuals in charge of cloud compliance to understand the organization's past?

A. To determine the current state of the organization's compliance
B. To determine the risk profile of the organization
C. To address any open findings from previous external audits
D. To verify whether the measures implemented from the lessons learned are effective

Answer: A

Explanation:
Understanding the organization??s past is crucial for individuals in charge of cloud compliance, particularly to address any open findings from previous external audits. This historical perspective is essential because it allows the compliance team to identify recurring issues, understand the context of past non-compliances, and ensure that corrective actions have been taken and are effective. It also helps in anticipating potential future compliance challenges based on past trends and patterns.
References = The importance of understanding an organization??s past for cloud compliance is supported by best practices in cloud security and compliance, which emphasize the need for continuous improvement and learning from past experiences to enhance security measures123.

NEW QUESTION 87
When mapping controls to architectural implementations, requirements define:

A. control objectives.
B. control activities.
C. guidelines.
D. policies.

Answer: B

Explanation:
Requirements define control activities, which are the actions, processes, or mechanisms that are implemented to achieve the control objectives1. Control objectives are the targets or desired conditions to be met that are designed to ensure that policy intent is met2. Guidelines are the recommended practices or advice that provide flexibility in how to implement a policy, standard, or control3. Policies are the statements of management??s intent that establish the direction, purpose, and scope of an organization??s internal control system4.
References:
? COSO – Control Activities - Deloitte1, section on Control Activities
? Words Matter - Understanding Policies, Control Objectives, Standards ??2, section on Control Objectives
? Understanding Policies, Control Objectives, Standards, Guidelines ??3, section on Guidelines
? Internal Control Handbook4, section on Policies

NEW QUESTION 88
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 92
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
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 100
Which of the following is a KEY benefit of using the Cloud Controls Matrix (CCM)?

A. CCM uses a specific control for Infrastructure as a Service (IaaS).
B. CCM maps to existing security standards, best practices, and regulations.
C. CCM V4 is an improved version from CCM V3.0.1.
D. CCM utilizes an ITIL framework to define the capabilities needed to manage the IT services and security services.

Answer: B

Explanation:
The Cloud Controls Matrix (CCM) by the Cloud Security Alliance provides a comprehensive control framework that aligns with industry standards, regulations, and best practices, offering a structured approach for cloud security and compliance management. This mapping capability makes it highly valuable in cloud audits as noted in the CCAK, which relies on CCM for its comprehensive applicability in regulatory compliance and security (referenced in CSA CCM V4 documentation and ISACA CCAK content).

NEW QUESTION 104
Which of the following standards is designed to be used by organizations for cloud services that intend to select controls within the process of implementing an information security management system based on ISO/IEC 27001?

A. ISO/IEC 27002
B. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
C. NISTSP 800-146
D. ISO/IEC 27017:2015

Answer: D

Explanation:
ISO/IEC 27017:2015 is a standard that provides guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002, as well as additional controls with implementation guidance that specifically relate to cloud services1. ISO/IEC 27017:2015 is designed to be used by organizations for cloud services that intend to select controls within the process of implementing an information security management system based on ISO/IEC 27001, which is the international standard for information security management systems1. ISO/IEC 27017:2015 can help organizations to establish, implement, maintain and continually improve their information security in the cloud environment, as well as to demonstrate compliance with contractual and legal obligations1.
ISO/IEC 27002 is a code of practice for information security controls that provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining information security management systems2. However, ISO/IEC 27002 does not provide specific guidance for cloud services, which is why ISO/IEC 27017:2015 was developed as an extension to ISO/IEC 27002 for cloud services1.
Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is a set of security controls that provides organizations with a detailed understanding of security concepts and principles that are aligned to the cloud model. The CCM is not a standard, but rather a framework that can be used to assess the overall security risk of a cloud provider. The CCM can also be mapped to other standards, such as ISO/IEC 27001 and ISO/IEC 27017:2015, to facilitate compliance and assurance activities.
NIST SP 800-146 is a publication from the National Institute of Standards and Technology (NIST) that provides an overview of cloud computing, its characteristics, service models, deployment models, benefits, challenges and considerations. NIST SP 800-146 is not a standard, but rather a reference document that can help organizations to understand the basics of cloud computing and its implications for information security. NIST SP 800-146 does not provide specific guidance or controls for cloud services, but rather refers to other standards and frameworks, such as ISO/IEC 27001 and CSA CCM, for more detailed information on cloud security. References :=
? ISO/IEC 27017:2015 - Information technology — Security techniques ??
? ISO/IEC 27017:2015(en), Information technology ? Security techniques ??
? ISO 27017 Certification - Cloud Security Services | NQA
? An introduction to ISO/IEC 27017:2015 - 6clicks
? ISO/IEC 27017:2015 - Information technology — Security techniques ??
? [Cloud Controls Matrix | Cloud Security Alliance]
? [NIST Cloud Computing Synopsis and Recommendations]

NEW QUESTION 109
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 confidentiality, integrity, and availability of the information system.
B. Determine the impact on the physical and environmental security of the organization, excluding informational assets.
C. Determine the impact on the controls that were selected by the organization to respond to identified risks.
D. Determine the impact on the financial, operational, compliance, and reputation of the organization.

Answer: A

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

? Threat identification: Identify the relevant threats from the CSA Top Threats reports that may affect the scope of the analysis.
? Technical impact identification: Determine the impact on confidentiality, integrity, and availability of the information system caused by each threat. Confidentiality refers to the protection of data from unauthorized access or disclosure. Integrity refers to the protection of data from unauthorized modification or deletion. Availability refers to the protection of data and services from disruption or denial.
? Business impact identification: Determine the impact on the business objectives and operations caused by each threat, such as financial loss, reputational damage, legal liability, or regulatory compliance.
? Risk assessment: Assess the likelihood and severity of each threat based on the technical and business impacts, and prioritize the threats according to their risk level.
? Risk treatment: Select and implement appropriate risk treatment options for each threat, such as avoidance, mitigation, transfer, or acceptance.
The technical impact identification step is important because it helps to measure the extent of damage or harm that each threat can cause to the information system and its components. This step also helps to align the technical impacts with the business impacts and to support the risk assessment and treatment steps.
References := CCAK Study Guide, Chapter 4: A Threat Analysis Methodology for Cloud Using CCM, page 81

NEW QUESTION 110
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 114
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 118
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 122
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 123
In relation to testing business continuity management and operational resilience, an auditor should review which of the following database documentation?

A. Database backup and replication guidelines
B. System backup documentation
C. Incident management documentation
D. Operational manuals

Answer: A

Explanation:
Database backup and replication guidelines are essential for ensuring the availability and integrity of data in the event of a disruption or disaster. They describe how the data is backed up, stored, restored, and synchronized across different locations and platforms. An auditor should review these guidelines to verify that they are aligned with the business continuity objectives, policies, and procedures of the organization and the cloud service provider. The auditor should also check that the backup and replication processes are tested regularly and that the results are documented and reported. References:
? ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 96
? Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM) v4.0, 2021, BCR-01: Business Continuity Planning/Resilience

NEW QUESTION 124
During an audit, it was identified that a critical application hosted in an off-premises cloud is not part of the organization's disaster recovery plan (DRP). Management stated that it is responsible for ensuring the cloud service provider has a plan that is tested annually. What should be the auditor's NEXT course of action?

A. Review the contract and DR capability.
B. Plan an audit of the provider.
C. Review the security white paper of the provider.
D. Review the provider's audit reports.

Answer: A

Explanation:
The auditor??s next course of action should be to review the contract and DR capability of the cloud service provider. The contract should specify the roles and responsibilities of both parties regarding disaster recovery, as well as the service level agreements (SLAs) and recovery time objectives (RTOs) for the critical application. The DR capability should demonstrate that the cloud service provider has a plan that is aligned with the organization??s requirements and expectations, and that it is tested annually and validated by independent auditors. The auditor should also verify that the organization has a process to monitor and review the cloud service provider??s performance and compliance with the contract and SLAs.
Planning an audit of the provider (B) may not be feasible or necessary, as the auditor may not have access to the provider??s environment or data, and may not have the authority or expertise to conduct such an audit. The auditor should rely on the provider??s audit reports and certifications to assess their compliance with relevant standards and regulations. Reviewing the security white paper of the provider © may not be sufficient or relevant, as the security white paper may not cover the specific aspects of disaster recovery for the critical application, or may not reflect the current state of the provider??s security controls and practices. The security white paper may also be biased or outdated, as it is produced by the provider themselves.
Reviewing the provider??s audit reports (D) may be helpful, but not enough, as the audit reports may not address the specific requirements and expectations of the organization for disaster recovery, or may not cover the latest changes or incidents that may affect the provider??s DR capability. The audit reports may also have limitations or qualifications that may affect their reliability or validity. References :=
? Audit a Disaster Recovery Plan | AlertFind
? ISACA Introduces New Audit Programs for Business Continuity/Disaster ??
? How to Maintain and Test a Business Continuity and Disaster Recovery Plan

NEW QUESTION 128
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 129
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 133
Which of the following helps an organization to identify control gaps and shortcomings in the context of cloud computing?

A. Walk-through peer review
B. Periodic documentation review
C. User security awareness training
D. Monitoring effectiveness

Answer: B

Explanation:
Periodic documentation review is a critical process that helps organizations identify control gaps and shortcomings, particularly in the context of cloud computing. This process involves regularly examining the documentation of processes, controls, and policies to ensure they are up-to-date and effective. It allows an organization to verify that the controls are operating as intended and to discover any areas where the controls may not fully address the organization??s requirements or the unique risks associated with cloud services. By conducting these reviews, organizations can maintain compliance with relevant regulations and standards, and ensure continuous improvement in their cloud security posture.
References = The significance of periodic documentation review is highlighted in cloud auditing and security best practices, as outlined by the Cloud Security Alliance (CSA) and the Certificate of Cloud Auditing Knowledge (CCAK) program12. These resources emphasize the importance of regular reviews as part of a comprehensive cloud governance and compliance strategy.

NEW QUESTION 135
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 140
Which of the following is an example of availability technical impact?

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

Answer: C

Explanation:
A distributed denial of service (DDoS) attack renders the customer??s cloud inaccessible for 24 hours is an example of availability technical impact. Availability is the protection of data and services from disruption or denial, and it is one of the three dimensions of information security, along with confidentiality and integrity. Availability technical impact refers to the extent of damage or harm that a threat can cause to the availability of the information system and its components, such as servers, networks, applications, and data. A DDoS attack is a malicious attempt to overwhelm a target system with a large volume of traffic or requests from multiple sources, making it unable to respond to legitimate requests or perform its normal functions. A DDoS attack can cause a significant availability technical impact by rendering the customer??s cloud inaccessible for a prolonged period of time, resulting in loss of productivity, revenue, customer satisfaction, and reputation. References := CCAK Study Guide, Chapter 4: A Threat Analysis Methodology for Cloud Using CCM, page 81; What is a DDoS Attack? | Cloudflare

NEW QUESTION 144
The MAIN limitation of relying on traditional cloud compliance assurance approaches such as SOC2 attestations is that:

A. they can only be performed by skilled cloud audit service providers.
B. they are subject to change when the regulatory climate changes.
C. they provide a point-in-time snapshot of an organization's compliance posture.
D. they place responsibility for demonstrating compliance on the vendor organization.

Answer: C

Explanation:
Traditional cloud compliance assurance approaches such as SOC2 attestations have the main limitation of providing a point-in-time snapshot of an organization??s compliance posture. This means that they only reflect the state of the organization??s security and compliance controls at a specific date or period, which may not be representative of the current or future state. Cloud environments are dynamic and constantly changing, and so are the threats and risks that affect them. Therefore, relying on traditional cloud compliance assurance approaches may not provide sufficient or timely assurance that the organization??s cloud services and data are adequately protected and compliant with the relevant requirements and standards.12
To overcome this limitation, some organizations adopt continuous cloud compliance assurance approaches, such as continuous monitoring, auditing, and reporting. These approaches enable the organization to collect, analyze, and report on the security and compliance status of its cloud environment in near real-

time, using automated tools and processes. Continuous cloud compliance assurance approaches can help the organization to identify and respond to any changes, issues, or incidents that may affect its cloud security and compliance posture, and to maintain a high level of trust and transparency with its stakeholders, customers, and regulators.34
References := What is SOC 2? Complete Guide to SOC 2 Reports | CSA1; Guidance on cloud security assessment and authorization - ITSP.50.105 - Canadian Centre for Cyber Security2; Continuous Compliance: The Future of Cloud Security | CloudCheckr3; Continuous Compliance: How to Automate Cloud Security Compliance4

NEW QUESTION 147
An organization is using the Cloud Controls Matrix (CCM) to extend its IT governance in the cloud. Which of the following is the BEST way for the organization to take advantage of the supplier relationship feature?

A. Filter out only those controls directly influenced by contractual agreements.
B. Leverage this feature to enable the adoption of the Shared Responsibility Model.
C. Filter out only those controls having a direct impact on current terms of service (TOS) andservice level agreement (SLA).
D. Leverage this feature to enable a smarter selection of the next cloud provider.

Answer: D

Explanation:
The best way for the organization to take advantage of the supplier relationship feature of the Cloud Controls Matrix (CCM) is to leverage this feature to enable a smarter selection of the next cloud provider. The supplier relationship feature is a column in the CCM spreadsheet that indicates whether a control is influenced by contractual agreements between the cloud service provider and the cloud customer. This feature can help the organization to identify and compare the security and compliance capabilities of different cloud providers, as well as to negotiate and customize the terms of service (TOS) and service level agreements (SLA) according to their needs and requirements123.
The other options are not the best ways to use the supplier relationship feature. Option A, filter out only those controls directly influenced by contractual agreements, is not a good way to use the feature because it would exclude other important controls that are not influenced by contractual agreements, but still relevant for cloud security and governance. Option B, leverage this feature to enable the adoption of the Shared Responsibility Model, is not a good way to use the feature because the Shared Responsibility Model is defined by another column in the CCM spreadsheet, which indicates whether a control is applicable to the cloud service provider or the cloud customer. Option C, filter out only those controls having a direct impact on current TOS and SLA, is not a good way to use the feature because it would exclude other controls that may have an indirect or potential impact on the TOS and SLA, or that may be subject to change or negotiation in the future. References :=
? What is CAIQ? | CSA - Cloud Security Alliance1
? Understanding the Cloud Control Matrix | CloudBolt Software3
? Cloud Controls Matrix (CCM) - CSA2

NEW QUESTION 152
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 155
Which of the following are independent assessment organizations that verify cloud providers' security implementations and provide the overall risk posture of a cloud environment for a FedRAMP security authorization decision?

A. FedRAMP Program Management Office (FedRAMP PMO)
B. American Association of Laboratory Accreditation (A2LA)
C. Third-party Assessment Organizations (3PAOs)
D. FedRAMP Joint Authorization Boards (JABs)

Answer: C

NEW QUESTION 157
Supply chain agreements between a cloud service provider and cloud customers should, at a minimum, include:

A. regulatory guidelines impacting the cloud customer.
B. audits, assessments, and independent verification of compliance certifications withagreement terms.
C. the organizational chart of the provider.
D. policies and procedures of the cloud customer

Answer: B

Explanation:

Supply chain agreements between a cloud service provider and cloud customers should, at a minimum, include audits, assessments, and independent verification of compliance certifications with agreement terms. This is because cloud services 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 important for the cloud customers to have visibility and assurance of the performance and compliance of the cloud providers and their sub- providers. Audits, assessments, and independent verification of compliance certifications are methods to evaluate the effectiveness of the controls and processes implemented by the cloud providers and their sub-providers to meet the agreement terms. These methods can help the cloud customers to identify any gaps or risks in the supply chain and to take corrective actions if needed. This is part of the Cloud Control Matrix (CCM) domain COM- 04: Audit Assurance & Compliance, which states that "The organization should have a policy and procedures to conduct audits and assessments of cloud services and data to verify compliance with applicable regulatory frameworks, contractual obligations, and industry standards."12 References := CCAK Study Guide, Chapter 3: Cloud Compliance Program, page 551; Practical Guide to Cloud Service Agreements Version 2.02

NEW QUESTION 159
What aspect of Software as a Service (SaaS) functionality and operations would the cloud customer be responsible for and should be audited?

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

Answer: C

Explanation:
Access controls are the aspect of Software as a Service (SaaS) functionality and operations that the cloud customer is responsible for and should be audited. Access controls refer to the methods and techniques that verify the identity and access rights of users or devices that access or use the SaaS application and its data. Access controls may include credentials, policies, roles, permissions, tokens, multifactor authentication, single sign-on, etc. The cloud customer is responsible for ensuring that only authorized and legitimate users or devices can access or use the SaaS application and its data, as well as for protecting the confidentiality, integrity, and availability of their data. The cloud customer should also monitor and audit the access and usage of the SaaS application and its data, as well as any incidents or issues that may affect them123.
Source code reviews (A) are not the aspect of SaaS functionality and operations that the cloud customer is responsible for and should be audited. Source code reviews refer to the processes and practices that examine the source code of software applications or systems to identify errors, bugs, vulnerabilities, or inefficiencies that may affect their quality, functionality, or security. Source code reviews are mainly under the responsibility of the cloud service provider, as they own and operate the software applications or systems that deliver SaaS services. The cloud customer has no access or control over these aspects123.
Patching (B) is not the aspect of SaaS functionality and operations that the cloud customer
is responsible for and should be audited. Patching refers to the processes and practices that ensure the security, reliability, and performance of the cloud infrastructure, platform, or software. Patching involves the use of updates or fixes to address vulnerabilities, bugs, errors, or exploits that may compromise or affect the functionality of the cloud components. Patching is mainly under the responsibility of the cloud service provider, as they own and operate the cloud infrastructure, platform, or software. The cloud customer has limited or no access or control over these aspects123.
Vulnerability management (D) is not the aspect of SaaS functionality and operations that the cloud customer is responsible for and should be audited. Vulnerability management refers to the processes and practices that identify, assess, treat, monitor, and report on the risks that affect the security posture of an organization or a domain. Vulnerability management involves the use of tools or techniques to scan, analyze, prioritize, remediate, or mitigate vulnerabilities that may expose an organization or a domain to threats or attacks. Vulnerability management is mainly under the responsibility of the cloud service
provider, as they own and operate the cloud infrastructure, platform, or software. The cloud customer has limited or no access or control over these aspects123.
References :=
? Cloud Audits: A Guide for Cloud Service Providers - Cloud Standards ??
? Cloud Audits: A Guide for Cloud Service Customers - Cloud Standards ??
? Cloud Auditing Knowledge: Preparing for the CCAK Certificate Exam

NEW QUESTION 161
Which of the following enables auditors to conduct gap analyses of what a cloud service provider offers versus what the customer requires?

A. Using a standardized control framework
B. The experience gained over the years
C. Understanding the customer risk profile
D. The as-is and to-be enterprise architecture (EA

Answer: A

Explanation:
Using a standardized control framework enables auditors to conduct gap analyses of what a cloud service provider (CSP) offers versus what the customer requires. A standardized control framework is a set of guidelines, best practices, and criteria that help to evaluate and improve the security, privacy, and compliance of cloud computing environments. Examples of standardized control frameworks include ISO/IEC 27001/27002/27017/27018, NIST SP 800-53, CSA Cloud Controls Matrix (CCM), COBIT,
etc. By using a standardized control framework, auditors can compare the CSP??s policies, procedures, and practices with the customer??s expectations and requirements, and identify any gaps or discrepancies that may pose risks or issues. A gap analysis can help the auditors to provide recommendations and suggestions to the CSP and the customer on how to close the gaps and enhance the quality and performance of the cloud services12. References:
? Cloud Controls Matrix (CCM) - CSA
? Cloud Computing Audit Program - ISACA

NEW QUESTION 162
In a multi-level supply chain structure where cloud service provider A relies on other sub cloud services, the provider should ensure that any compliance requirements relevant to the provider are:

A. passed to the sub cloud service providers based on the sub cloud service providers' geographic location.
B. passed to the sub cloud service providers.
C. treated as confidential information and withheld from all sub cloud service providers.
D. treated as sensitive information and withheld from certain sub cloud service providers.

Answer: A

Explanation:

In a multi-level supply chain structure, the cloud service provider should ensure that any compliance requirements relevant to the provider are passed to the sub cloud service providers, regardless of their geographic location. This is because the sub cloud service providers may have access to or process the data of the provider??s customers, and thus may affect the compliance status of the provider. The provider should also monitor and verify the compliance of the sub cloud service providers on a regular basis. This is part of the Cloud Control Matrix (CCM) domain COM-01: Regulatory Frameworks, which states that "The organization should identify and comply with applicable regulatory frameworks, contractual obligations, and industry standards."1 References := CCAK Study Guide, Chapter 3: Cloud Compliance Program, page 51

NEW QUESTION 163
Which of the following cloud service provider activities MUST obtain a client's approval?

A. Destroying test data
B. Deleting subscription owner accounts
C. Deleting test accounts
D. Deleting guest accounts

Answer: B

Explanation:
Deleting subscription owner accounts is an activity that MUST obtain a client??s approval in the context of cloud service provider activities. Subscription owner accounts are critical as they hold the ownership and control over the resources and services within a cloud subscription. Deleting these accounts can have significant implications, including loss of access, control, and potential data loss. Therefore, it is essential for a cloud service provider to seek explicit approval from the client before proceeding with such an action to ensure transparency, maintain trust, and avoid any unintended consequences.
References:
? Microsoft Trust Center, Cloud Services Due Diligence Checklist1.
? Google Cloud, What is a Cloud Service Provider?2.
? Partner Center, CSP agreements, price lists, and offers3.
? Microsoft Azure, How to choose a cloud service provider4.
? FCA, FG16/5 Guidance for firms outsourcing to the ??cloud?? and other third-party IT services

NEW QUESTION 166
What is a sign that an organization has adopted a shift-left concept of code release cycles?

A. Large entities with slower release cadences and geographically dispersed systems
B. Incorporation of automation to identify and address software code problems early
C. A waterfall model remove resources through the development to release phases
D. Maturity of start-up entities with high-iteration to low-volume code commits

Answer: B

Explanation:
The shift-left concept of code release cycles is a practice that aims to integrate testing, quality, and performance evaluation early in the software development life cycle, often before any code is written. This helps to find and prevent defects, improve quality, and enable faster delivery of secure software. One of the key aspects of the shift- left concept is the incorporation of automation to identify and address software code problems early, such as using continuous integration, continuous delivery, and continuous testing tools. Automation can help reduce manual errors, speed up feedback loops, and increase efficiency and reliability123
The other options are not correct because:
? Option A is not correct because large entities with slower release cadences and geographically dispersed systems are more likely to face challenges in adopting the shift-left concept, as they may have more complex and legacy systems, dependencies, and processes that hinder agility and collaboration. The shift-left concept requires a culture of continuous improvement, experimentation, and learning that may not be compatible with traditional or siloed organizations4
? Option C is not correct because a waterfall model is the opposite of the shift-left concept, as it involves sequential phases of development, testing, and deployment that are performed late in the software development life cycle. A waterfall model does not allow for early detection and correction of defects, feedback, or changes, and can result in higher costs, delays, and risks5
? Option D is not correct because maturity of start-up entities with high-iteration to low-volume code commits is not a sign of the shift-left concept, but rather a sign of the agile or lean software development methodologies. These methodologies focus on delivering value to customers by delivering working software in short iterations or sprints, with frequent feedback and adaptation. While these methodologies can support the shift-left concept by enabling faster testing and delivery cycles, they are not equivalent or synonymous with it6
References: 1: AWS. What is DevSecOps? - Developer Security Operations Explained -
AWS. [Online]. Available: 4. [Accessed: 14-Apr-2023]. 2: Dynatrace. Shift left vs shift right: A DevOps mystery solved - Dynatrace news. [Online]. Available: 2. [Accessed: 14-Apr-
2023]. 3: BMC Software. Shift Left Testing: What, Why & How To Shift Left – BMC
Software | Blogs. [Online]. Available: 3. [Accessed: 14-Apr-2023]. 4: GitLab. How to shift left with continuous integration | GitLab. [Online]. Available: 4. [Accessed: 14-Apr-2023]. 5: DZone. DevOps and The Shift-Left Principle - DZone. [Online]. Available: 5. [Accessed: 14- Apr-2023]. 6: Devopedia. Shift Left - Devopedia. [Online]. Available: 6. [Accessed: 14-Apr- 2023].

NEW QUESTION 170
Which of the following is MOST important to ensure effective cloud application controls are maintained in an organization?

A. Control self-assessment (CSA)
B. Third-party vendor involvement
C. Exception reporting
D. Application team internal review

Answer: C

Explanation:
Exception reporting is crucial for maintaining effective cloud application controls within an organization. It involves monitoring and reporting deviations from standard operating procedures, which can indicate potential security issues. This proactive approach allows organizations to address vulnerabilities promptly before they can be exploited. Exception reporting is a key component of a robust security posture, as it provides real-time insights into the operational effectiveness of controls and helps maintain compliance with security policies.
References = The importance of exception reporting is highlighted in best practices for cloud security, which emphasize the need for continuous monitoring and immediate response to any anomalies detected in cloud applications

NEW QUESTION 175
"Policies and procedures shall be established, and supporting business processes and technical measures implemented, for maintenance of several items ensuring continuity and availability of operations and support personnel." Which of the following types of controls BEST matches this control description?

A. System development maintenance
B. Operations maintenance
C. System maintenance
D. Equipment maintenance

Answer: B

NEW QUESTION 176
It is MOST important for an auditor to be aware that an inventory of assets within a cloud environment:

A. should be mapped only if discovered during the audit.
B. is not fundamental for the security management program, as this is a cloud service.
C. can be a misleading source of data.
D. is fundamental for the security management program

Answer: D

Explanation:
It is most important for an auditor to be aware that an inventory of assets within a cloud environment is fundamental for the security management program. An inventory of assets is a list of all the hardware, software, data, and services that are owned, used, or managed by an organization in the cloud. An inventory of assets helps the organization to identify, classify, and prioritize its cloud resources and to implement appropriate security controls and policies to protect them. An inventory of assets also helps the organization to comply with relevant regulations, standards, and contracts that may apply to its cloud environment.12
An auditor should be aware of the importance of an inventory of assets in the cloud because it provides a baseline for assessing the security posture and compliance status of the organization??s cloud environment. An auditor can use the inventory of assets to verify that the organization has a clear and accurate understanding of its cloud resources and their characteristics, such as location, ownership, configuration, dependencies, vulnerabilities, and risks. An auditor can also use the inventory of assets to evaluate whether the organization has implemented adequate security measures and processes to protect its cloud resources from threats and incidents. An auditor can also use the inventory of assets to identify any gaps or weaknesses in the organization??s security management program and to provide recommendations for improvement.34
References := Why is IT Asset Inventory Management Critical? - Fresh Security1; Use asset inventory to manage your resources?? security posture2; The importance of asset inventory in cybersecurity3; The Importance Of Asset Inventory In Cyber Security And CMDB - Visore4

NEW QUESTION 180
After finding a vulnerability in an Internet-facing server of an organization, a cybersecurity criminal is able to access an encrypted file system and successfully manages to overwrite parts of some files with random data. In reference to the Top Threats Analysis methodology, how would the technical impact of this incident be categorized?

A. As an integrity breach
B. As an availability breach
C. As a confidentiality breach
D. As a control breach

Answer: A

Explanation:
As an integrity breach. The technical impact of this incident can be categorized as an integrity breach, which refers to the effect of a cloud security incident on the protection of data from unauthorized modification or deletion. Integrity is one of the three security properties of an information system, along with confidentiality and availability. The incident described in the question involves a cybersecurity criminal finding a vulnerability in an Internet-facing server of an organization, accessing an encrypted file system, and overwriting parts of some files with random data. This is a type of data tampering or corruption attack that affects the accuracy and reliability of the data. The fact that the file system was encrypted does not prevent the integrity breach, as the attacker did not need to decrypt or read the data, but only to overwrite it. The integrity breach can have serious consequences for the organization, such as data loss, data inconsistency, data recovery costs, and loss of trust.
The other options are not correct categories for the technical impact of this incident. Option B, as an availability breach, is incorrect because availability refers to the protection of data and services from disruption or denial, which is not the case in this incident. Option C, as a confidentiality breach, is incorrect because confidentiality refers to the protection of data from unauthorized access or disclosure, which is not the case in this incident. Option D, as a control breach, is incorrect because control refers to the ability to manage or influence the behavior or outcome of a system or process, which is not a security property of an information system. References: =
? Top Threats Analysis Methodology - CSA1
? Top Threats Analysis Methodology - Cloud Security Alliance2
? OWASP Risk Rating Methodology | OWASP Foundation3
? OEE Factors: Availability, Performance, and Quality | OEE4
? The Effects of Technological Developments on Work and Their

NEW QUESTION 183
Which of the following would be the MOST critical finding of an application security and DevOps audit?

A. Certifications with global security standards specific to cloud are not reviewed, and the impact of noted findings are not assessed.
B. Application architecture and configurations did not consider security measures.
C. Outsourced cloud service interruption, breach, or loss of stored data occurred at the cloud service provider.
D. The organization is not using a unified framework to integrate cloud compliance with regulatory requirements

Answer: B

Explanation:
According to the web search results, the most critical finding of an application security and DevOps audit would be that the application architecture and configurations did not consider security measures. This finding indicates a serious lack of security by design and security by default principles, which are essential

for ensuring the confidentiality, integrity, and availability of the application and its data . If the application architecture and configurations are not secure, they could expose the application to various threats and vulnerabilities, such as unauthorized access, data breaches, denial-of-service attacks, injection attacks, cross-site scripting attacks, and others . This finding could also result in non-compliance with relevant security standards and regulations, such as ISO 27001, PCI DSS, GDPR, and others . Therefore, this finding should be addressed with high priority and urgency by implementing appropriate security measures and controls in the application architecture and configurations.
The other options are not as critical as option B. Option A is a moderate finding that indicates a lack of awareness and assessment of the global security standards specific to cloud, such as ISO 27017, ISO 27018, CSA CCM, NIST SP 800-53, and others . This finding could affect the security and compliance of the cloud services used by the application, but it does not directly impact the application itself. Option C is a severe finding that indicates a major incident that occurred at the cloud service provider level, such as a service interruption, breach, or loss of stored data. This finding could affect the availability,
confidentiality, and integrity of the application and its data, but it is not caused by the application itself. Option D is a minor finding that indicates a lack of efficiency and consistency in integrating cloud compliance with regulatory requirements. This finding could affect the compliance posture of the application and its data, but it does not directly impact the security or functionality of the application. References:
? [Application Security Best Practices - OWASP]
? [DevSecOps: What It Is and How to Get Started - ISACA]
? [Cloud Security Standards: What to Expect & What to Negotiate - CSA]
? [Cloud Computing Security Audit - ISACA]
? [Cloud Computing Incident Response - ISACA]
? [Cloud Compliance: A Framework for Using Cloud Services While Maintaining Compliance - ISACA]

NEW QUESTION 186
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CCAK Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CCAK Product From:

https://www.2passeasy.com/dumps/CCAK/

Money Back Guarantee

CCAK Practice Exam Features:

* CCAK Questions and Answers Updated Frequently

* CCAK Practice Questions Verified by Expert Senior Certified Staff

* CCAK Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CCAK Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year