High Pass-Rate Relevant CCAK Exam Dumps Offer You The Best Latest Braindumps Sheet | Certificate of Cloud Auditing Knowledge

What's more, part of that Exam4PDF CCAK dumps now are free: https://drive.google.com/open?id=1dXKdC5Ym6T2Hc-P-u4kpPq-ODDFR3yPP

The privacy protection of users is an eternal issue in the internet age. Many illegal websites will sell users' privacy to third parties, resulting in many buyers are reluctant to believe strange websites. But you don't need to worry about it at all when buying our CCAK study materials. We assure you that we will never sell users' information because it is damaging our own reputation. In addition, when you buy our CCAK Study Materials, our website will use professional technology to encrypt the privacy of every user to prevent hackers from stealing.

The CCAK Certification program is administered by the Information Systems Audit and Control Association (ISACA), a global non-profit organization that is dedicated to the advancement of information systems governance and security. The program is designed to provide professionals with a solid foundation in cloud security auditing and to equip them with the knowledge and skills required to carry out cloud security audits effectively.

>> Relevant CCAK Exam Dumps <<

2025 Realistic ISACA Relevant CCAK Exam Dumps Pass Guaranteed Quiz

Our CCAK training guide always promise the best to service the clients. Carefully testing and producing to match the certified quality standards of CCAK exam materials, we have made specific statistic researches on the CCAK practice materials. And the operation system of our CCAK practice materials can adapt to different consumer groups. Facts speak louder than words. Through years' efforts, our CCAK exam preparation has received mass favorable reviews because the 99% pass rate is the powerful proof of trust of the public.

For more info read reference

Isaca CCAK Exam Reference

ISACA Certificate of Cloud Auditing Knowledge Sample Questions (Q206-Q211):

NEW QUESTION # 206
Which of the following is MOST important to manage risk from cloud vendors who might accidentally introduce unnecessary risk to

an organization by adding new features to their solutions?

- A. Deploying new features using cloud orchestration tools
- B. Performing prior due diligence of the vendor
- C. Establishing responsibility in the vendor contract
- D. Implementing service level agreements (SLAs) around changes to baseline configurations

Answer: D

Explanation:
Implementing service level agreements (SLAs) around changes to baseline configurations is the most important way to manage risk from cloud vendors who might accidentally introduce unnecessary risk to an organization by adding new features to their solutions. A service level agreement (SLA) is a contract or a part of a contract that defines the expected level of service, performance, and quality that a cloud vendor will provide to an organization. An SLA can also specify the roles and responsibilities, the communication channels, the escalation procedures, and the penalties or remedies for non-compliance12.
Implementing SLAs around changes to baseline configurations can help an organization to manage the risk from cloud vendors who might add new features to their solutions without proper testing, validation, or notification. Baseline configurations are the standard or reference settings for a system or a network that are used to measure and maintain its security and performance. Changes to baseline configurations can introduce new vulnerabilities, errors, or incompatibilities that can affect the functionality, availability, or security of the system or network34. Therefore, an SLA can help an organization to ensure that the cloud vendor follows a change management process that includes steps such as risk assessment, impact analysis, approval, documentation, notification, testing, and rollback. An SLA can also help an organization to monitor and verify the changes made by the cloud vendor and to report and resolve any issues or incidents that may arise from them.
The other options are not the most effective ways to manage the risk from cloud vendors who might add new features to their solutions. Option A, deploying new features using cloud orchestration tools, is not a good way to manage the risk because cloud orchestration tools are used to automate and coordinate the deployment and management of complex cloud services and resources. Cloud orchestration tools do not address the issue of whether the new features added by the cloud vendor are necessary, secure, or compatible with the organization's system or network. Option B, performing prior due diligence of the vendor, is not a good way to manage the risk because prior due diligence is a process that involves evaluating and verifying the background, reputation, capabilities, and compliance of a potential cloud vendor before entering into a contract with them. Prior due diligence does not address the issue of how the cloud vendor will handle changes to their solutions after the contract is signed. Option C, establishing responsibility in the vendor contract, is not a good way to manage the risk because establishing responsibility in the vendor contract is a process that involves defining and assigning the roles and obligations of both parties in relation to the cloud service delivery and performance. Establishing responsibility in the vendor contract does not address the issue of how the cloud vendor will communicate and coordinate with the organization about changes to their solutions. Reference := What is an SLA? Best practices for service-level agreements | CIO1 Service Level Agreements - Cloud Security Alliance2 What is Baseline Configuration? - Definition from Techopedia3 Baseline Configuration - Cloud Security Alliance4 Change Management - Cloud Security Alliance Incident Response - Cloud Security Alliance What is Cloud Orchestration? - Definition from Techopedia Due Diligence - Cloud Security Alliance Contractual Security Requirements - Cloud Security Alliance

NEW QUESTION # 207
Which of the following aspects of risk management involves identifying the potential reputational and financial harm when an incident occurs?

- A. Mitigation
- B. Residual risk
- C. Impact analysis
- D. Likelihood

Answer: C

Explanation:
Impact analysis is the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Impact analysis is the process of estimating the consequences or effects of a risk event on the business objectives, operations, processes, or functions. Impact analysis helps to measure and quantify the severity or magnitude of the risk event, as well as to prioritize and rank the risks based on their impact. Impact analysis also helps to determine the appropriate level of response and mitigation for each risk event, as well as to allocate the necessary resources and budget for risk management123.
Likelihood (A) is not the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Likelihood is the aspect of risk management that involves estimating the probability or frequency of a risk event occurring. Likelihood is the process of assessing and evaluating the factors or causes that may trigger or influence a risk event, such

as threats, vulnerabilities, assumptions, uncertainties, etc. Likelihood helps to measure and quantify the chance or possibility of a risk event happening, as well as to prioritize and rank the risks based on their likelihood123.
Mitigation (B) is not the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Mitigation is the aspect of risk management that involves reducing or minimizing the likelihood or impact of a risk event. Mitigation is the process of implementing and applying controls or actions that can prevent, avoid, transfer, or accept a risk event, depending on the risk appetite and tolerance of the organization. Mitigation helps to improve and enhance the security and resilience of the organization against potential risks, as well as to optimize the cost and benefit of risk management123.
Residual risk is not the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Residual risk is the aspect of risk management that involves measuring and monitoring the remaining or leftover risk after mitigation. Residual risk is the process of evaluating and reviewing the effectiveness and efficiency of the mitigation controls or actions, as well as identifying and addressing any gaps or issues that may arise. Residual risk helps to ensure that the actual level of risk is aligned with the desired level of risk, as well as to update and improve the risk management strategy and plan123. References :=
* Risk Analysis: A Comprehensive Guide | SafetyCulture
* Risk Assessment and Analysis Methods: Qualitative and Quantitative - ISACA
* Risk Management Process - Risk Management | Risk Assessment | Risk ...

NEW QUESTION # 208
What areas should be reviewed when auditing a public cloud?

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

Answer: D

Explanation:
Identity and access management (IAM) and data protection are the areas that should be reviewed when auditing a public cloud, as they are the key aspects of cloud security and compliance that affect both the cloud service provider and the cloud service customer. IAM and data protection refer to the methods and techniques that ensure the confidentiality, integrity, and availability of data and resources in the cloud environment. IAM involves the use of credentials, policies, roles, permissions, and tokens to verify the identity and access rights of users or devices. Data protection involves the use of encryption, backup, recovery, deletion, and retention to protect data from unauthorized access, modification, loss, or disclosure123.
Patching and configuration (A) are not the areas that should be reviewed when auditing a public cloud, as they are not the key aspects of cloud security and compliance that affect both the cloud service provider and the cloud service customer. Patching and configuration refer 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. Configuration involves the use of settings or parameters to customize or optimize the functionality of the cloud components. Patching and configuration are mainly under the responsibility of the cloud service provider, as they own and operate the cloud infrastructure, platform, or software. The cloud service customer has limited or no access or control over these aspects123.
Vulnerability management and cyber security reviews (B) are not the areas that should be reviewed when auditing a public cloud, as they are not specific or measurable aspects of cloud security and compliance that can be easily audited or tested. Vulnerability management and cyber security reviews refer 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. Cyber security reviews involve the use of tools or techniques to evaluate, measure, benchmark, or improve the security capabilities or maturity of an organization or a domain. Vulnerability management and cyber security reviews are general or broad terms that encompass various aspects of cloud security and compliance, such as IAM, data protection, patching, configuration, etc. Therefore, they are not specific or measurable areas that can be audited or tested individually123.
Source code reviews and hypervisor (D) are not the areas that should be reviewed when auditing a public cloud, as they are not relevant or accessible aspects of cloud security and compliance for most cloud service customers. 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. Hypervisor refers to the software that allows the creation and management of virtual machines on a physical server. Source code reviews and hypervisor are mainly under the responsibility of the cloud service provider, as they own and operate the software applications or systems that deliver cloud services. The cloud service customer has no access or control over these aspects123. Reference := Cloud Audits: A Guide for Cloud Service Providers - Cloud Standards ...
Cloud Audits: A Guide for Cloud Service Customers - Cloud Standards ...

NEW QUESTION # 209
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. The organization is not using a unified framework to integrate cloud compliance with regulatory requirements.
- C. Outsourced cloud service interruption, breach, or loss of stored data occurred at the cloud service provider.
- D. Application architecture and configurations did not consider security measures.

Answer: D

Explanation:
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 would indicate that the application is vulnerable to various threats and attacks, such as data breaches, unauthorized access, injection, cross-site scripting, denial-of-service, etc. This finding would also imply that the application does not comply with the security standards and best practices for cloud services, such as ISO/IEC 27017:20151, CSA Cloud Controls Matrix2, or NIST SP 800-1463. This finding would require immediate remediation and improvement of the application security posture, as well as the implementation of security controls and tests throughout the DevOps process.
Certifications with global security standards specific to cloud are not reviewed, and the impact of noted findings are not assessed (A) would be a significant finding of an application security and DevOps audit, but not the most critical one. This finding would indicate that the organization is not aware or informed of the security requirements and expectations for cloud services, as well as the gaps or issues that may affect their compliance or performance. This finding would require regular review and analysis of the certifications with global security standards specific to cloud, such as ISO/IEC 270014, CSA STAR Certification, or FedRAMP Authorization, as well as the assessment of the impact of noted findings on the organization's risk profile and business objectives.
Outsourced cloud service interruption, breach, or loss of stored data occurred at the cloud service provider (B) would be a serious finding of an application security and DevOps audit, but not the most critical one. This finding would indicate that the cloud service provider failed to ensure the availability, confidentiality, and integrity of the cloud services and data that they provide to the organization. This finding would require investigation and resolution of the root cause and impact of the incident, as well as the implementation of preventive and corrective measures to avoid recurrence. This finding would also require review and verification of the contractual terms and conditions between the organization and the cloud service provider, as well as the service level agreements (SLAs) and recovery time objectives (RTOs) for the cloud services.
The organization is not using a unified framework to integrate cloud compliance with regulatory requirements
would be an important finding of an application security and DevOps audit, but not the most critical one.
This finding would indicate that the organization is not following a consistent and systematic approach to manage and monitor its cloud compliance with regulatory requirements, such as GDPR, HIPAA, PCI DSS, etc. This finding would require adoption and implementation of a unified framework to integrate cloud compliance with regulatory requirements, such as COBIT, NIST Cybersecurity Framework, or CIS Controls, as well as the alignment and integration of these frameworks with the DevOps process.

NEW QUESTION # 210
Which of the following types of risk is associated specifically with the use of multi-cloud environments in an organization?

- A. Risk of service reliability and uptime
- B. Risk of unauthorized access to customer and business data
- C. Risk of supply chain visibility and validation
- D. Risk of reduced visibility and control

Answer: D

Explanation:
In multi-cloud environments, organizations use cloud services from multiple providers. This can lead to challenges in maintaining visibility and control over the data and services due to the varying management tools, processes, and security controls across different providers. The complexity of managing multiple service models and the reliance on different cloud service providers can reduce an organization's ability to monitor and control its resources effectively, thus increasing the risk of reduced visibility and control.
References = The information aligns with the principles outlined in the CCAK materials, which emphasize the unique challenges of auditing the cloud, including ensuring the right controls for confidentiality, integrity, and accessibility, and mitigating risks such as those associated with multi-cloud environments12.

NEW QUESTION # 211
.....

Latest CCAK Braindumps Sheet: https://www.exam4pdf.com/CCAK-dumps-torrent.html

- Quiz 2025 ISACA High Hit-Rate Relevant CCAK Exam Dumps □ Search for （ CCAK ） and obtain a free download on ▸ www.torrentvalid.com ◂ □Dumps CCAK PDF
- CCAK Valid Exam Tutorial □ Dumps CCAK Vce □ CCAK Test Guide □ Search for □ CCAK □ and download it for free immediately on [www.pdfvce.com] □CCAK Practice Exam Fee
- Quiz 2025 ISACA High Hit-Rate Relevant CCAK Exam Dumps □ Copy URL " www.exams4collection.com " open and search for " CCAK " to download for free □Reliable CCAK Test Testking
- CCAK Actual Test Pdf □ CCAK Frenquent Update □ CCAK Study Tool ☯ Download □ CCAK □ for free by simply entering 【 www.pdfvce.com 】 website □CCAK Valid Exam Tutorial
- CCAK Frenquent Update □ Exam CCAK Discount □ Exam CCAK Answers □ Enter □ www.real4dumps.com □ and search for ➠ CCAK □ to download for free □Exam CCAK Discount
- Relevant CCAK Exam Dumps | Trustable Certificate of Cloud Auditing Knowledge 100% Free Latest Braindumps Sheet □ Search for ☀ CCAK □☀□ and download it for free immediately on ➤ www.pdfvce.com □ □Dumps CCAK Vce
- Quiz 2025 ISACA CCAK: Certificate of Cloud Auditing Knowledge – The Best Relevant Exam Dumps □ The page for free download of " CCAK " on " www.examcollectionpass.com " will open immediately □CCAK Frenquent Update
- CCAK Study Tool □ Reliable CCAK Test Testking □ Dumps CCAK Vce □ ➥ www.pdfvce.com □ is best website to obtain ▸ CCAK ◂ for free download □CCAK Pass Guaranteed
- CCAK Instant Access □ New CCAK Dumps Ebook □ Dumps CCAK PDF □ Easily obtain 【 CCAK 】 for free download through □ www.prep4sures.top □ □CCAK Frenquent Update
- CCAK Pass Guaranteed □ Dumps CCAK PDF □ Latest CCAK Braindumps □ Go to website □ www.pdfvce.com □ open and search for ➡ CCAK □□□ to download for free □Reliable CCAK Test Testking
- CCAK Actual Questions □ CCAK Actual Questions □ Latest CCAK Braindumps □ Search for □ CCAK □ on ▸ www.pdfdumps.com ◂ immediately to obtain a free download □New CCAK Dumps Ebook
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.x7cq.vip, study.stcs.edu.np, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, mindlybody.com, mobile-maths.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2025 ISACA CCAK dumps are available on Google Drive shared by Exam4PDF: https://drive.google.com/open?id=1dXKdC5Ym6T2Hc-P-u4kpPq-ODDFR3yPP