Free Questions for CCAK by dumpshq

Shared by Hutchinson on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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.

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

Question 2

Question Type: **MultipleChoice**

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?

Options:

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.

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

Question 3

Question Type: MultipleChoice

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

Options:

A- Examine the cloud provider's certifications and ensure the scope is appropriate.

B- Document the requirements and responsibilities within the customer contract

C- Interview the cloud security team and ensure compliance.

D- Pen test the cloud service provider to ensure compliance.

Answer:

A

Explanation:

The most effective way to ensure a vendor is compliant with the agreed-upon cloud service is to examine the cloud provider's certifications and ensure the scope is appropriate.Certifications are independent attestations of the cloud provider's compliance with various standards, regulations, and best practices related to cloud security, privacy, and governance1.They provide assurance to customers that the cloud provider has implemented adequate controls and processes to meet their contractual obligations and expectations2.However, not all certifications are equally relevant or comprehensive, so customers need to verify that the certifications cover the specific cloud service, region, and data type that they are using3.Customers should also review the certification reports or audit evidence to understand the scope, methodology, and results of the assessment4.

The other options are not as effective as examining the cloud provider's certifications.Documenting the requirements and responsibilities within the customer contract is an important step to establish the terms and conditions of the cloud service agreement, but it does not guarantee that the vendor will comply with them5. Customers need to monitor and verify the vendor's performance and compliance on an ongoing basis. Interviewing the cloud security team may provide some insights into the vendor's compliance practices, but it may not be sufficient or reliable without independent verification or documentation. Pen testing the cloud service provider may reveal some vulnerabilities or weaknesses in the vendor's security posture, but it may not cover all aspects of compliance or be authorized by the vendor. Pen testing should be done with caution and consent, as it may cause disruption or damage to the cloud service or violate the terms of service.

Cloud Compliance: What You Need To Know - Linford & Company LLP1, section on Cloud Compliance

Cloud Services Due Diligence Checklist | Trust Center2, section on Why Microsoft created the Cloud Services Due Diligence Checklist

The top cloud providers for government | ZDNET3, section on What is FedRAMP?

Cloud Computing Security Considerations | Cyber.gov.au4, section on Certification

Cloud Audits and Compliance: What You Need To Know - Linford & Company LLP5, section on Cloud Compliance Management

Cloud Services Due Diligence Checklist | Trust Center, section on How to use the checklist

Cloud Computing Security Considerations | Cyber.gov.au, section on Security governance

The top cloud providers for government | ZDNET, section on Penetration testing

Penetration Testing in AWS - Amazon Web Services (AWS), section on Introduction

Question 4

Question Type: **MultipleChoice**

During the cloud service provider evaluation process, which of the following BEST helps identify baseline configuration requirements?

Options:

A- Vendor requirements

B- Product benchmarks

C- Benchmark controls lists

D- Contract terms and conditions

Answer:

C

Explanation:

: During the cloud service provider evaluation process, benchmark controls lists BEST help identify baseline configuration requirements.Benchmark controls lists are standardized sets of security and compliance controls that are applicable to different cloud service models, deployment models, and industry sectors1.They provide a common framework and language for assessing and comparing the security posture and capabilities of cloud service providers2.They also help cloud customers to define their own security and compliance requirements and expectations based on best practices and industry standards3.

Some examples of benchmark controls lists are:

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM), which is a comprehensive list of 133 control objectives that cover 16 domains of cloud security4.

The National Institute of Standards and Technology (NIST) Special Publication 800-53, which is a catalog of 325 security and privacy controls for federal information systems and organizations, including cloud-based systems5.

The International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27017, which is a code of practice that provides guidance on 121 information security controls for cloud services based on ISO/IEC 270026.

CSA Security Guidance for Cloud Computing | CSA1, section on Identify necessary security and compliance requirements

Evaluation Criteria for Cloud Infrastructure as a Service - Gartner2, section on Security Controls

Checklist: Cloud Services Provider Evaluation Criteria | Synoptek3, section on Security

Cloud Controls Matrix | CSA4, section on Overview

NIST Special Publication 800-53 - NIST Pages5, section on Abstract

ISO/IEC 27017:2015(en), Information technology --- Security techniques ...6, section on Scope

What is vendor management?Definition from WhatIs.com7, section on Vendor management

What is Benchmarking?Definition from WhatIs.com8, section on Benchmarking

What is Terms and Conditions?Definition from WhatIs.com9, section on Terms and Conditions

Question 5

Question Type: **MultipleChoice**

When mapping controls to architectural implementations, requirements define:

Options:

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.

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

Question 6

Question Type: MultipleChoice

Which of the following is a detective control that may be identified in a Software as a Service (SaaS) service provider?

Options:

A- Data encryption

B- Incident management

C- Network segmentation

D- Privileged access monitoring

Answer:

D

Explanation:

A detective control is a type of internal control that seeks to uncover problems in a company's processes once they have occurred1.Examples of detective controls include physical inventory checks, reviews of account reports and reconciliations, as well as assessments of current controls1.Detective controls use platform telemetry to detect misconfigurations, vulnerabilities, and potentially malicious activity in the cloud environment2.

In a Software as a Service (SaaS) service provider, privileged access monitoring is a detective control that can help identify unauthorized or suspicious activities by users who have elevated permissions to access or modify cloud resources, data, or configurations.Privileged access monitoring can involve logging, auditing, alerting, and reporting on the actions performed by privileged users3. This can help detect security incidents, compliance violations, or operational errors in a timely manner and enable appropriate responses.

Data encryption, incident management, and network segmentation are examples of preventive controls, which are designed to prevent problems from occurring in the first place.Data encryption protects the confidentiality and integrity of data by transforming it into an unreadable format that can only be decrypted with a valid key1.Incident management is a process that aims to restore normal service operations as quickly as possible after a disruption or an adverse event4.Network segmentation divides a network into smaller subnetworks that have different access levels and security policies, reducing the attack surface and limiting the impact of a breach1.

Detective controls - SaaS Lens - docs.aws.amazon.com3, section on Privileged access monitoring

Detective controls | Cloud Architecture Center | Google Cloud2, section on Detective controls

Internal control: how do preventive and detective controls work?4, section on SaaS Solutions to Support Internal Control

Detective Control: Definition, Examples, Vs.Preventive Control1, section on What Is a Detective Control?