CLO-002$^{\text{Q\&As}}$

CompTIA Cloud Essentials+

QUESTION 1

A developer is leveraging a public cloud service provider to provision servers using the templates created by the company\\'s cloud engineer.

Which of the following does this BEST describe?

A. Subscription services

B. Containerization

C. User self-service

D. Autonomous environments

Correct Answer: C

Explanation: User self-service is a cloud computing feature that allows users to provision, manage, and terminate cloud resources on demand, without the need for human intervention or approval. User self-service enables users to access cloud services through an online control panel, a web portal, or an API. User self-service can improve the agility, efficiency, and scalability of cloud computing, as users can quickly and easily obtain the resources they need, when they need them, and pay only for what they use. User self- service can also reduce the workload and costs of the cloud service provider, as they do not have to manually process requests or allocate resources. In this scenario, a developer is leveraging a public cloud service provider to provision servers using the templates created by the company\\'s cloud engineer. This means that the developer can access the cloud provider\\'s web portal or API, select the desired template, and launch the server instance without waiting for approval or assistance from the cloud provider or the cloud engineer. This is an example of user self-service, as the developer can self-manage the cloud resources according to their needs. References:

1: What is On-Demand Self Service? - Definition from Techopedia

2: What is Self-Service Provisioning in Cloud? | CloudBolt Software CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 2: The Business Side of Cloud Computing, Section 2.1: Cloud Service Models3

QUESTION 2

A company purchased insurance due to the risks involved with a cloud migration project. Which of the following risk response strategies is this an example of?

A. Mitigation

B. Avoidance

C. Acceptance

D. Transference

Correct Answer: D

Explanation: Transference is a risk response strategy that involves shifting the responsibility or impact of a risk to a third party, such as an insurance company, a vendor, or a partner. By purchasing insurance, the company transferred the financial liability of the cloud migration project to the insurance provider, in case of any losses or damages.

Transference does not eliminate the risk, but it reduces the exposure of the company to the risk12. References: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 4: Risk Management, pages 104-105.

QUESTION 3

A business analyst is drafting a risk assessment.

Which of the following components should be included in the draft? (Choose two.)

A. Asset management

B. Database type

C. Encryption algorithms

D. Certificate name

E. Asset inventory

F. Data classification

Correct Answer: EF

Explanation: A risk assessment is a process of identifying, analyzing, and controlling hazards and risks within a situation or a place1. According to the CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), a risk assessment should include the following steps2: Identify the assets that are relevant to the scope of the assessment. Assets can be physical, such as hardware and software, or non-physical, such as data and information. Identify the threats and vulnerabilities that could affect the assets. Threats are sources of potential harm, such as natural disasters, cyberattacks, or human errors. Vulnerabilities are weaknesses or gaps in the security or protection of the assets, such as outdated software, misconfigured settings, or lack of encryption. Analyze the likelihood and impact of each threat-vulnerability pair. Likelihood is the probability of a threat exploiting a vulnerability, and impact is the severity of the consequences if that happens. The combination of likelihood and impact determines the level of risk for each pair. Evaluate the risks and prioritize them based on their level. Risks can be categorized as low, medium, high, or critical, depending on the organization\\'s risk appetite and tolerance. Risk appetite is the amount of risk that the organization is willing to accept, and risk tolerance is the degree of variation from the risk appetite that the organization can endure. Implement appropriate controls to mitigate or reduce the risks. Controls are measures or actions that can prevent, detect, or correct the occurrence or impact of a risk. Controls can be administrative, technical, or physical, and they can have different functions, such as preventive, detective, corrective, deterrent, or compensating. Based on these steps, two components that should be included in the draft of a risk assessment are asset inventory and data classification. Asset inventory is the process of identifying and documenting the assets that are within the scope of the assessment1. Data classification is the process of categorizing data based on its sensitivity, value, and criticality to the organization3. These components are essential for determining the potential risks and impacts that could affect the assets and data, and for applying the appropriate controls and protection levels.

https://www.comptia.org/training/books/cloud-essentials-clo-002-study-guide
https://books.google.com/books/about/CompTIA_Cloud_Essentials+_Certification.html?id= S2TNDwAAQBAJ

QUESTION 4

A project manager must inform the Chief Information Officer (CIO) of the additional resources necessary to migrate services to the cloud successfully.

Which of the following cloud assessments would be MOST appropriate to use for the recommendation?

A. Feasibility study

B. Gap analysis

C. Future requirements

D. Baseline report

Correct Answer: B

Explanation: A gap analysis is a process of comparing the current state and the desired state of a system or a process and identifying the gaps or differences between them. A gap analysis can help an organization to determine the steps and resources needed to achieve its goals and objectives. A gap analysis can be used for cloud migration to assess the readiness and suitability of the existing services and applications for the cloud, and to identify the gaps in terms of performance, security, functionality, compatibility, and cost. A gap analysis can also help to prioritize the migration tasks and to estimate the time and effort required for the migration1. The other options are not appropriate for the recommendation: Feasibility study: This is a process of evaluating the viability and benefits of a proposed project or solution. A feasibility study can help an organization to determine whether a project is worth pursuing, and to identify the potential risks and challenges involved. A feasibility study can be used for cloud migration to evaluate the benefits and drawbacks of moving to the cloud, and to compare different cloud service models and providers. A feasibility study can also help to define the scope and objectives of the migration project2. However, a feasibility study is not sufficient to inform the CIO of the additional resources necessary for the migration, as it does not provide a detailed analysis of the gaps and requirements of the existing services and applications. Future requirements: These are the needs and expectations of the organization and its stakeholders for the future state of the system or the process. Future requirements can help an organization to plan and design the system or the process to meet the changing demands and opportunities. Future requirements can be used for cloud migration to envision the desired outcomes and benefits of moving to the cloud, and to align the migration strategy with the business strategy and goals3. However, future requirements are not specific enough to inform the CIO of the additional resources necessary for the migration, as they do not provide a detailed analysis of the gaps and requirements of the existing services and applications. Baseline report: This is a document that records the current state and performance of the system or the process, and serves as a reference point for measuring the progress and improvement. A baseline report can help an organization to monitor and evaluate the system or the process, and to identify the areas of strength and weakness. A baseline report can be used for cloud migration to measure the performance and functionality of the existing services and applications, and to compare them with the cloud-based services and applications4. However, a baseline report is not comprehensive enough to inform the CIO of the additional resources necessary for the migration, as it does not provide a detailed analysis of the gaps and requirements of the existing services and applications. References: Gap Analysis for Cloud Migration Feasibility Study for Cloud Migration Future Requirements for Cloud Migration Baseline Report for Cloud Migration

QUESTION 5

A company is discontinuing its use of a cloud provider. Which of the following should the provider do to ensure there is no sensitive data stored in the company\\'s cloud?

A. Replicate the data.

B. Encrypt the data.

C. Lock in the data.

D. Sanitize the data.

Correct Answer: D

Explanation: Data sanitization is the process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device. Data sanitization is a security best practice and often a compliance requirement for sensitive or confidential data. Data sanitization ensures that the data cannot be recovered by any means, even by advanced forensic tools. Data sanitization can be done by overwriting, degaussing, or physically destroying the storage media. When a company discontinues its use of a cloud provider, the provider should sanitize the data to prevent any unauthorized access, leakage, or breach of the company\\'s data. References: CompTIA Cloud Essentials+ Certification Exam Objectives1, CompTIA Cloud Essentials+ Study Guide, Chapter 4: Cloud Storage2, Data sanitization for cloud storage3

QUESTION 6

Which of the following metrics defines how much data loss a company can tolerate?

A. RTO

B. TCO

C. MTTR

D. ROI

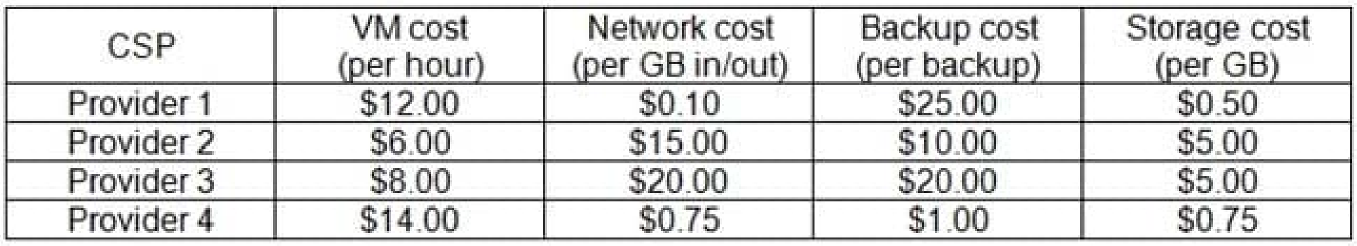
E. RPO

Correct Answer: E

Explanation: RPO stands for recovery point objective, which is the maximum amount of data loss that a company can tolerate in the event of a disaster, failure, or disruption. RPO is measured in time, from the point of the incident to the last valid backup of the data. RPO helps determine how frequently the company needs to back up its data and how much data it can afford to lose. For example, if a company has an RPO of one hour, it means that it can lose up to one hour\\'s worth of data without causing significant harm to the business. Therefore, it needs to back up its data at least every hour to meet its RPO. RPO is different from other metrics such as RTO, TCO, MTTR, and ROI. RTO stands for recovery time objective, which is the maximum amount of time that a company can tolerate for restoring its data and resuming its normal operations after a disaster. TCO stands for total cost of ownership, which is the sum of all the costs associated with acquiring, maintaining, and operating a system or service over its lifetime. MTTR stands for mean time to repair, which is the average time that it takes to fix a faulty component or system. ROI stands for return on investment, which is the ratio of the net profit to the initial cost of a project or investment. References: Recovery Point Objective: A Critical Element of Data Recovery - G2, What is a Recovery Point Objective? RPO Definition + Examples, Cloud Computing Pricing Models -CompTIA Cloud Essentials+ (CLO-002) Cert Guide

QUESTION 7

A startup company that provides streaming media services is considering a new CSP. The company sees an average volume of 5000TB daily and high QoS. It has received the following bids:



CSP	VM cost (per hour)	Network cost (per GB in/out)	Backup cost (per backup)	Storage cost (per GB)
Provider 1	$12.00	$0.10	$25.00	$0.50
Provider 2	$6.00	$15.00	$10.00	$5.00
Provider 3	$8.00	$20.00	$20.00	$5.00
Provider 4	$14.00	$0.75	$1.00	$0.75

Based on the information above, which of the following CSPs offers the MOST cost- effective solution for streaming?

A. Provider 1

B. Provider 2

C. Provider 3

D. Provider 4

Correct Answer: D

Explanation: The most cost-effective solution for streaming is the one that offers the lowest cost per GB for storage and network. In this case, Provider 4 offers the lowest cost per GB for storage ($0.10) and network ($0.01). Additionally, Provider 4 offers the lowest cost for backup ($5.00) and VM cost ($4.00 per hour). References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 4: Selecting Cloud Service Providers, page 85

QUESTION 8

Which of the following is related to data availability in the cloud?

A. Resiliency

B. Deduplication

C. Scalability

D. Elasticity

Correct Answer: A

Explanation: Data availability in the cloud refers to the ability of cloud services to provide continuous and uninterrupted access to data, even in the event of a network disruption or a disaster. Resiliency is the ability of a system to recover quickly from failures and restore normal operations. Resiliency is related to data availability in the cloud because it ensures that data is not lost or corrupted due to failures and that data can be accessed by users and applications without delays or errors. Deduplication, scalability, and elasticity are not directly related to data availability in the cloud, although they may have some impact on the performance and efficiency of cloud services. Deduplication is the process of eliminating redundant copies of data to save storage space and bandwidth. Scalability is the ability of a system to handle increasing or decreasing workloads by adding or removing resources. Elasticity is the ability of a system to automatically adjust the amount of resources based on the current demand. References: CompTIA Cloud Essentials+ CLO- 002 Study Guide, Chapter 2: Cloud Concepts, Section 2.3: Cloud Service Characteristics, Page 411

QUESTION 9

A company requires 24 hours\\' notice when a database is taken offline for planned maintenance. Which of the following policies provides the BEST guidance about notifying users?

A. Communication policy

B. Access control policy

C. Information security policy

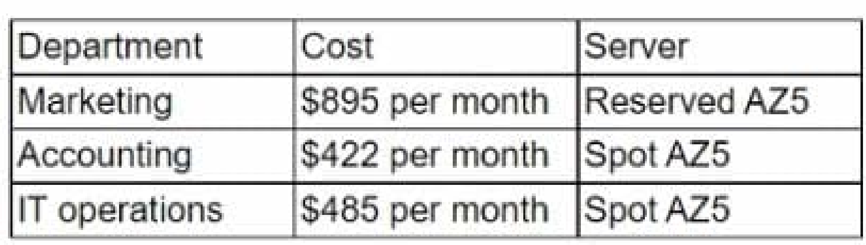
D. Risk management policy

Correct Answer: A

Explanation: A communication policy is a set of guidelines that defines how an organization communicates with its internal and external stakeholders, such as employees, customers, partners, and regulators. A communication policy typically covers topics such as the purpose, scope, methods, frequency, tone, and responsibilities of communication within and outside the organization. A communication policy also establishes the standards and expectations for communication quality, accuracy, timeliness, and security. A communication policy is essential for ensuring effective, consistent, and transparent communication across the organization and with its stakeholders. A communication policy can help to avoid misunderstandings, conflicts, and errors that may arise from poor or unclear communication. A communication policy can also help to enhance the reputation, trust, and credibility of the organization. A communication policy provides the best guidance about notifying users when a database is taken offline for planned maintenance, because it specifies how, when, and to whom such notifications should be sent. A communication policy can help to ensure that users are informed in advance, in a clear and courteous manner, about the reason, duration, and impact of the maintenance, and that they are updated on the progress and completion of the maintenance. A communication policy can also help to address any questions, concerns, or feedback that users may have regarding the maintenance. A communication policy can thus help to minimize the disruption and inconvenience caused by the maintenance, and to maintain a positive relationship with the users. A communication policy is different from the other policies listed in the question, which are not directly related to notifying users about planned maintenance. An access control policy defines the rules and procedures for granting or denying access to information systems and resources based on the identity, role, and privileges of the users. An information security policy outlines the principles and practices for protecting the confidentiality, integrity, and availability of information assets and systems from unauthorized or malicious use, disclosure, modification, or destruction. A risk management policy describes the process and criteria for identifying, assessing, prioritizing, mitigating, and monitoring the risks that may affect the organization\\'s objectives, operations, and performance. While these policies are important for ensuring the security and reliability of the database and the organization, they do not provide specific guidance about communicating with users about planned maintenance. References: Cloud Essentials+ CLO-002 Study Guide, Chapter 4: Cloud Service Management, Section 4.2: Explain aspects of change management within a cloud environment, p. 115. What is Cloud Communications? Your Getting Started Guide, Cloud Communications ?Defined. Cloud Computing Policy and Guidelines, 1. Introduction. Define corporate policy for cloud governance, Cloud-based IT policies. DEPARTMENT OF COMMUNICATIONS AND DIGITAL TECHNOLOGIES NO. 306 1 April 2021, 5. Function of cloud security policy and standards, Policy should always address.

QUESTION 10

A large enterprise has the following invoicing breakdown of current cloud consumption spend:



Department	Cost	Server
Marketing	$895 per month	Reserved AZ5
Accounting	$422 per month	Spot AZ5
IT operations	$485 per month	Spot AZ5

The level of resources consumed by each department is relatively similar. Which of the following is MOST likely affecting monthly costs?

A. The servers in use by the marketing department are in an availability zone that is generally expensive.

B. The servers in use by the accounting and IT operations departments are in different geographic zones with lower pricing.

C. The accounting and IT operations departments are choosing to bid on non-committed resources.

D. The marketing department likely stores large media files on its servers, leading to increased storage costs.

Correct Answer: D

Explanation: The marketing department likely stores large media files on its servers, leading to increased storage costs. This is because the marketing department is responsible for creating and distributing various types of digital content, such as videos, images, podcasts, and webinars, to promote the products and services of the enterprise. These media files tend to be large in size and require more storage space than other types of data, such as text documents or spreadsheets. Therefore, the marketing department consumes more storage resources than the other departments, which increases the monthly cloud costs for the enterprise. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 3: Cloud Service and Delivery Models, Section 3.2: Cloud Storage, Page 97

QUESTION 11

Which of the following are the appropriate responses to risks?

A. Mitigate, accept, avoid, validate

B. Migrate, accept, avoid, transfer

C. Mitigate, accept, avoid, transfer

D. Migrate, accept, avoid, validate

Correct Answer: C

Explanation: According to the CompTIA Cloud Essentials+ CLO-002 Study Guide, there are four common risk response types: avoid, share or transfer, mitigate, and accept1. These are the appropriate responses to risks, depending on the risk type, assessment, and attitude. The other options are incorrect because they include terms that are not valid risk responses. For example, migrate is not a risk response, but a cloud deployment strategy. Validate is not a risk response, but a quality assurance technique. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 4: Cloud Security, Section 4.2: Cloud Security Concepts, Page 153.

QUESTION 12

Which of the following describes the contractually allowed downtime for a cloud-hosted application?

A. SOW

B. SLA

C. SOP

D. SOA

Correct Answer: B

Explanation: An SLA (service level agreement) is a contract between a cloud service provider and a cloud customer that defines the expected level of service, performance, availability, and reliability of the cloud service. An SLA also specifies the contractually allowed downtime for a cloud-hosted application, which is the maximum amount of time that the application can be unavailable or inaccessible without violating the SLA. The contractually allowed downtime is usually expressed as a percentage of uptime, such as 99.9% or 99.99%, which corresponds to a certain number of hours or minutes per year, month, week, or day. For example, an SLA with 99.9% uptime means that the cloud service can be down for up to 8.76 hours per year, or 43.8 minutes per month, or 10.1 minutes per week, or 1.44 minutes per day. If the cloud service provider fails to meet the SLA, the cloud customer may be entitled to compensation or other remedies, such as credits, refunds, or termination of the contract. References: CompTIA Cloud Essentials+ CLO-002 Certification Study Guide, page 27-28; CompTIA Cloud Essentials+ Certification Training, CertMaster Learn for Cloud Essentials+, Module 2: Business Principles of Cloud Environments, Lesson 2.4: Cloud Service Agreements, Topic 2.4.2: Service Level Agreements

QUESTION 13

Which of the following is commonly used to forecast market trends?

A. Serverless computing

B. Data warehouse

C. Machine learning

D. Accelerated computing

Correct Answer: C

Explanation: Machine learning is a branch of artificial intelligence that enables computers to learn from data and make predictions or decisions without being explicitly programmed. Machine learning can be used to forecast market trends by analyzing historical and current data, identifying patterns and relationships, and generating models that can extrapolate future outcomes. Machine learning can also adapt to changing data and environments, and improve its accuracy and performance over time1. The other options are not commonly used to forecast market trends: Serverless computing: This is a type of cloud computing that allows customers to run applications or functions without managing or provisioning servers. Serverless computing can reduce the operational and infrastructure costs, and improve the scalability and availability of the applications or functions. However, serverless computing is not directly related to forecasting market trends, although it can be used to deploy or run machine learning models or applications2. Data warehouse: This is a centralized repository that stores structured and historical data from various sources, such as databases, applications, or files. Data warehouse can support business intelligence and analytics, and provide consistent and reliable data for reporting and decision making. However, data warehouse is not a forecasting method, but rather a data storage and integration system, that can be used as an input for machine learning or other forecasting methods3. Accelerated computing: This is a type of computing that uses specialized hardware, such as graphics processing units (GPUs) or field-programmable gate arrays (FPGAs), to accelerate the performance of certain applications or tasks, such as machine learning, gaming, or video processing. Accelerated computing can enhance the speed and efficiency of the applications or tasks, and reduce the power consumption and costs. However, accelerated computing is not a forecasting method, but rather a computing platform, that can be used to support or enable machine learning or other forecasting methods4. References: Machine Learning for Forecasting Market Trends Serverless Computing for Machine Learning Data Warehouse for Business Intelligence and Analytics Accelerated Computing for Machine Learning

QUESTION 14

An organization is determining an acceptable amount of downtime. Which of the following aspects of cloud design should the organization evaluate?

A. RPO

B. RTO

C. ERP

D. TCO

Correct Answer: B

Explanation: RTO stands for Recovery Time Objective, which is the time frame within which an IT resource must fully recover from a disruptive event1. RTO is a measure of the acceptable amount of downtime that an organization can tolerate in case of a disaster or a failure2. RTO helps an organization to plan and design its cloud backup and disaster recovery strategy, as it determines how quickly the cloud services and applications need to be restored to resume normal business operations2. RTO also helps an organization to estimate the potential costs and losses associated with downtime, and to balance them with the costs and resources required for recovery2. RTO is different from RPO, which stands for Recovery Point Objective, and is the acceptable amount of data loss that an organization can tolerate in case of a disaster or a failure1. RPO helps an organization to plan and design its cloud backup frequency and retention policy, as it determines how much data needs to be backed up and how often2. RPO also helps an organization to estimate the potential costs and losses associated with data loss, and to balance them with the costs and resources required for backup2. ERP stands for Enterprise Resource Planning, which is a type of software system that integrates and automates various business processes and functions, such as accounting, inventory, human resources, customer relationship management, and more3. ERP is not directly related to cloud design or downtime, although some ERP systems can be deployed on the cloud or use cloud services3. TCO stands for Total Cost of Ownership, which is a financial estimate that considers all the direct and indirect costs associated with acquiring and operating an asset or a service over its lifetime. TCO is a useful metric for comparing different cloud solutions and providers, as it helps an organization to evaluate the true costs and benefits of cloud adoption. TCO is not directly related to cloud design or downtime, although downtime can affect the TCO of a cloud solution by increasing the costs and reducing the benefits. References: 2: CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 3: Cloud Planning, Section 3.2: Cloud Adoption, Subsection 3.2.3: Recovery Point Objective and Recovery Time Objective; 1: phoenixNAP, RTO vs RPO Understanding The Key Difference; 3: Investopedia, Enterprise Resource Planning (ERP); : CompTIA Cloud Essentials+ Certification Study Guide, Second Edition (LO-002), Chapter 2: Cloud Concepts, Section 2.2: Cloud Economics, Subsection 2.2.1: Total Cost of Ownership

QUESTION 15

A business analyst is reviewing a software upgrade plan. The plan mentions the term "hash" value. Which of the following BEST represents what this term implies?

A. Non-repudiation of data

B. Integrity of data

C. Confidentiality of data

D. Availability of data

Correct Answer: B

Explanation: A hash value is a unique code that is generated by applying a mathematical algorithm to a piece of data. Hash values are used to ensure the integrity of data, which means that the data has not been altered or corrupted in any way. By comparing the hash value of the original data with the hash value of the received or stored data, one can verify that the data is identical and has not been tampered with. Hash values can also be used for digital signatures, which provide non-repudiation of data, meaning that the sender or owner of the data cannot deny its authenticity or origin. However, hash values alone do not provide confidentiality or availability of data, which are other aspects of data security. Confidentiality means that the data is protected from unauthorized access or disclosure, and availability means that the data is accessible and usable when needed. Hash values do not encrypt or hide the data, nor do they prevent data loss or downtime. References: CompTIA Cloud Essentials+ CLO-002 Study Guide, Chapter 5: Cloud Security Principles, Section 5.2: Data Security Concepts, Page 1471 and Ensuring Data Integrity with Hash Codes - .NET |

Microsoft Learn