CERTSHOP

ISC2 CCSP® - Quiz Questions with Answers

Domain 1: Cloud Concepts, Architecture and Design

1.

A multinational conglomerate company manufactures smart appliances that include washing machines and espresso machines. Some of their products have ended up being used by a consulting firm. These products are in the buildings (lights and such) and in the breakrooms (refrigerators). These products are connected to the network and are sending their logs to the Security Information and Event Manager (SIEM). An analysist in the Security Operations Center (SOC) has been analysing an Indication of Compromise (IoC). The IoC indicates correctly that an attack has occurred by a bad actor that has compromised a virtual desktop that then led to a compromise of the database.

What does this say about the smart appliances?

- **True negative**
- True positive
- False negative
- False positive

Correct answer: True negative

To understand true negatives, it is essential to grasp the concept of a confusion matrix, which is a table that summarizes the performance of a classification model. The confusion matrix consists of four elements:

1. ***True Positives (TP)**: The model correctly predicts positive outcomes when the actual outcomes are indeed positive.*
2. ***True Negatives (TN)**: The model correctly predicts negative outcomes when the actual outcomes are indeed negative.*
3. ***False Positives (FP)**: The model incorrectly predicts positive outcomes when the actual outcomes are negative.*
4. ***False Negatives (FN)**: The model incorrectly predicts negative outcomes when the actual outcomes are positive.*

Because there is nothing that the analyst sees about the smart appliances and there is a compromise between the virtual desktop and the database, there is no problem with the smart appliances. Therefore, it is true that there are no (negative) IoCs regarding the smart appliances being attacked.

2.

AWS Lambda is BEST described by which of the following cloud service models?

FaaS

SaaS

IaaS

PaaS

Correct answer: FaaS

Cloud services are typically provided under three main service models:

- *Software as a Service (SaaS): Under the SaaS model, the cloud provider offers the customer access to a complete application developed by the cloud provider. Webmail services like Google Workspace and Microsoft 365 are examples of SaaS offerings.*
- *Platform as a Service (PaaS): In a PaaS model, the cloud provider offers the customer a managed environment where they can build and deploy applications. The cloud provider manages compute, data storage, and other services for the application.*
- *Infrastructure as a Service (IaaS): In IaaS, the cloud provider offers an environment where the customer has access to various infrastructure building blocks. AWS, which allows customers to deploy virtual machines (VMs) or use block data storage in the cloud, is an example of an IaaS platform.*

Function as a Service (FaaS) is a form of PaaS in which the customer creates individual functions that can run in the cloud. Examples include AWS Lambda, Microsoft Azure Functions, and Google Cloud Functions.

3.

Abigail is designing the infrastructure of Identity and Access Management (IAM) for their future Platform as a Service (PaaS) environment. As she is setting up identities, she knows that which of the following is true of roles?

Roles are temporarily assumed by another identity

Roles are permanently assumed by a user or group

Roles are assigned to specific users permanently and occasionally assumed

Roles are the same as user identities

Correct answer: Roles are temporarily assumed by another identity

Roles are not the same as they are in traditional data centers. Roles are in a way similar to traditional roles in that they allow a user or group a certain amount of access. The group is closer to what we traditionally called roles in Role Based Access Control (RBAC). In the cloud, roles are assumed temporarily. You can assume roles in a variety of ways, but, again, they are temporary.

The user is not permanently assigned a specific role. A user will log in as their user identity, then assume a role. This is temporary (e.g., for 15 hours or only the life of that session).

Note the distinction between assigning and assuming roles — you might have access to certain permissions, but you only use the role and those permissions occasionally.

An additional resource for your review/study is on the AWS website. Look for the user guide regarding roles.

4.

Which technology provides a distributed and secure data management solution that leverages the cloud while maintaining data privacy and control?

Private

Public

Consortium

Hybrid

Correct answer: Private

There are four types of blockchain: private, public, consortium, and hybrid.

Private blockchains are restricted to a specific group of participants who are granted access and permission to the network. They are typically used within organizations or consortia where participants trust each other and require more control over the network. Private blockchains offer higher transaction speeds and privacy but sacrifice decentralization compared to public blockchains.

Public blockchains, such as Bitcoin and Ethereum, are open to anyone and allow anyone to participate in the network, verify transactions, and create new blocks. They are decentralized and provide a high level of transparency and security. Public blockchains use consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), to validate transactions and secure the network.

Consortium blockchains are a hybrid of public and private blockchains. They are operated by a consortium or a group of organizations that have a shared interest in a particular industry or use case. Consortium blockchains provide a controlled and permissioned environment, while still allowing multiple entities to participate in the consensus and decision-making process.

Permissioned blockchains require users to have permission to join and participate in the network. They are typically used in enterprise settings where access control and governance are critical. Permissioned blockchains offer faster transaction speeds and are more scalable than public blockchains, but they sacrifice some decentralization and censorship resistance.

The hybrid blockchain approach allows organizations to leverage the benefits of decentralization, transparency, and immutability from public blockchains while maintaining control, privacy, and scalability through private components. It offers a

flexible solution that can cater to specific business requirements and regulatory considerations.

5.

Which of the following is a strategy for maintaining operations during a business-disrupting event?

BCP

DRP

BIA

SAMM

Correct answer: BCP

A business continuity plan (BCP) is a strategy for maintaining operations during a business-disrupting event. A disaster recovery plan (DRP) is a strategy for restoring normal operations after such an event.

Business impact analysis (BIA) focuses on identifying the business impact if an asset, system, or process is degraded or lost.

An OWASP software assurance maturity model (SAMM) can help organizations assess the security of their current development practices.

6.

Which of the following cloud deployment models is NOT defined in NIST SP 800-145?

Multi-cloud

Public cloud

Hybrid cloud

Private cloud

Correct answer: Multi-cloud

NIST SP 800-145 defines four cloud deployment models. They are:

- *Private cloud: In private clouds, the cloud customer builds their own cloud in-house or has a provider do so for them. Private clouds have dedicated servers, making them more secure but also more expensive.*
- *Public cloud: Public clouds are multi-tenant environments where multiple cloud customers share the same infrastructure managed by a third-party provider.*
- *Hybrid cloud: Hybrid cloud deployments mix both public and private cloud infrastructure. This allows data and applications to be hosted on the cloud that makes the most sense for them.*
- *Community cloud: A community cloud is essentially a private cloud used by a group of related organizations rather than a single organization. It could be operated by that group or a third party, such as FedRAMP-compliant cloud environments operated by cloud service providers.*

Multi-cloud environments use cloud services from multiple different cloud providers. They enable customers to take advantage of price differences or optimizations offered by different providers. While multi-cloud is growing in popularity, it is not currently defined in NIST SP 800-145.

7.

An organization is looking to balance concerns about data security with the desire to leverage the scalability and cost savings of the cloud. Which of the following cloud models is the BEST choice for this?

Hybrid Cloud

Private Cloud

Community Cloud

Public Cloud

Correct answer: Hybrid Cloud

Cloud services are available under a few different deployment models, including:

- *Private Cloud: In private clouds, the cloud customer builds their own cloud in-house or has a provider do so for them. Private clouds have dedicated servers, making them more secure but also more expensive.*
- *Public Cloud: Public clouds are multi-tenant environments where multiple cloud customers share the same infrastructure managed by a third-party provider.*
- *Hybrid Cloud: Hybrid cloud deployments mix both public and private cloud infrastructure. This allows data and applications to be hosted on the cloud that makes the most sense for them. For example, sensitive data can be stored on the private cloud, while less-sensitive applications can take advantage of the benefits of the public cloud.*
- *Multi-Cloud: Multi-cloud environments use cloud services from multiple different cloud providers. This enables customers to take advantage of price differences or optimizations offered by different providers.*
- *Community Cloud: A community cloud is essentially a private cloud used by a group of related organizations rather than a single organization. It could be operated by that group or a third party, such as FedRAMP-compliant cloud environments operated by cloud service providers.*

8.

If either Structured Query Language (SQL) injection or cross-site scripting vulnerabilities exist within any Software as a Service (SaaS) implementation, customers' data is at risk. Of the following, what is the BEST method for preventing this type of security risk?

Input validation

Bounds checking

Output validation

Data sanitization

Correct answer: Input validation

Cross-Site Scripting (XSS) occurs on webpages. SQL injection can occur on a webpage or any form that a user fills out that has a SQL database on the backend. Both of these can be discovered or prevented if input validation is done. SQL commands are very recognizable, and the software can be coded to look for and block any inputs from the user that are SQL commands. XSS is also detectable within the HTML of a webpage. If the other page that a user is directed to is a different domain, it can be blocked, or at least notify the user that they are being directed to another site.

Bounds checking is a technique used in computer programming to ensure that an index or pointer accessing an array or data structure remains within the valid range of the data it is accessing. It is primarily used to prevent buffer overflows, array out-of-bounds errors, and other related vulnerabilities that can lead to security vulnerabilities or program crashes.

Output validation, also known as output verification or output validation testing, is a process in software development that involves verifying and validating the correctness, integrity, and quality of the output produced by a system, application, or module.

Data sanitization is the process of removing data from the media in some manner, such as overwrites or physical destruction.

9.

Which of the following emerging technologies improves portability in the cloud?

Containers

Fog Computing

TEEs

Edge Computing

Correct answer: Containers

Cloud computing is closely related to many emerging technologies. Some examples include:

- *Containers: Containerization packages an application with all of the dependencies that it needs to run in a single package. This container can then be moved to any platform running the container software, including cloud platforms.*
- *Edge and Fog Computing: Edge and fog computing move computations from centralized servers to devices at the network edge, enabling faster responses and less usage of bandwidth and computational power by cloud servers. Edge computing performs computing on IoT devices, while fog computing uses gateways at the edge to collect data from these devices and perform computation there.*
- *Confidential Computing: While data is commonly encrypted at rest and in transit, it is often decrypted while in use, which creates security concerns. Confidential computing involves the use of trusted execution environments (TEEs) that protect and isolate sensitive data from potential threats while in use.*

10.

Which cloud service role negotiates relationships between cloud customers' relationships with cloud providers?

Cloud service broker

Cloud auditor

Cloud service partner

Cloud service user

Correct answer: Cloud service broker

The cloud service broker is responsible for negotiating relationships between the customer and the provider. They would be considered independent of both.

Cloud service partners are defined in ISO/IEC 17788 as a party that is engaged in support of, or auxiliary to, either the cloud service customer or the cloud service provider.

The cloud auditor is defined in ISO/IEC 17788 as a partner that audits the provision and use of cloud services.

The cloud auditors and cloud service broker would be considered cloud service partners. The partner is a more generic role.

The cloud service customer is defined in ISO/IEC 17788 as a natural person associated with the cloud service customer.

11.

A cloud service provider has published a SOC 2 report. Which of the following cloud considerations is this MOST relevant to?

Auditability

Governance

Regulatory Oversight

Security

Correct answer: Auditability

When deploying cloud infrastructure, organizations must keep various security-related considerations in mind, including:

- *Security: Data and applications hosted in the cloud must be secured just like in on-prem environments. Three key considerations are the CIA triad of confidentiality, integrity, and availability.*
- *Privacy: Data hosted in the cloud should be properly protected to ensure that unauthorized users can't access the data of customers, employees, and other third parties.*
- *Governance: An organization's cloud infrastructure is subject to various laws, regulations, corporate policies, and other requirements. Governance manages cloud operations in a way that ensures compliance with these various constraints.*
- *Auditability: Cloud computing outsources the management of a portion of an organization's IT infrastructure to a third party. A key contractual clause is ensuring that the cloud customer can audit (directly or indirectly) the cloud provider to ensure compliance with contractual, legal, and regulatory obligations. A SOC 2 report shows that a cloud service provider meets certain requirements regarding the protection of the customer's data.*
- *Regulatory Oversight: An organization's responsibility for complying with various regulations (PCI DSS, GDPR, etc.) also extends to its use of third-party services. Cloud customers need to be able to ensure that cloud providers are compliant with applicable laws and regulations.*

12.

A cloud information security manager is building the policies and associated documents for handling cloud assets. She is currently detailing how assets will be understood or listed so that access can be controlled, alerts can be created, and billing can be tracked.

What concept enables this?

- **Tags**
- Values
- Datatype
- Identifier

Correct answer: Tags

Tags are pervasive in cloud deployments. A plan must be built for the corporation on how to tag assets. If it is not done consistently, it is not helpful. A tag is made up of two pieces, a key and a value. For example, in the tag "cert:CCSP," "cert" is the key, and "CSSP" is the value. Tags are also sometimes called "labels" (e.g., in Kubernetes)

A datatype is a data categorization.

Tags are technically a type of identifier. However, an identifier is too generic of an answer in this case.

13.

Which of the following network security controls is used to manage access to certain critical or sensitive resources?

Network Security Groups

Traffic Inspection

Geofencing

Zero Trust Network

Correct answer: Network Security Groups

Network security controls that are common in cloud environments include:

- *Network Security Groups: Network security groups (NSGs) limit access to certain resources, such as firewalls or sensitive VMs or databases. This makes it more difficult for an attacker to access these resources during their attacks.*
- *Traffic Inspection: In the cloud, traffic monitoring can be complex since traffic is often sent directly to virtual interfaces. Many cloud environments have traffic mirroring solutions that allow an organization to see and analyze all traffic to its cloud-based resources.*
- *Geofencing: Geofencing limits the locations from which a resource can be accessed. This is a helpful security control in the cloud, which is accessible from anywhere.*
- *Zero Trust Network: Zero trust networks apply the principle of least privilege, where users, applications, systems, etc. are only granted the access and permissions that they need for their jobs. All requests for access to resources are individually evaluated, so an entity can only access those resources for which they have the proper permissions.*

14.

Which of the following is NOT an example of a functional security requirement in the cloud?

Availability

Portability

Interoperability

Vendor lock-in

Correct answer: Availability

Functional requirements refer to aspects of a system, device, or user that are necessary for it to do its job. Common examples of functional security requirements in the cloud are portability, interoperability, and vendor lock-in. Availability is a nonfunctional requirement.

15.

Rashid has been working with his customer to understand the Indication of Compromise (IoC) that they have seen within their Security Information and Event Manager (SIEM). The logs show that a bad actor infiltrated their organization through a phishing email. Once the bad actor was in, they traversed the network till they gained access to a firewall. Once they were in the firewall, the bad actor assumed the role the firewall had to access the database. The database was then copied by the bad actor.

This is an example of which type of threat?

- **Data breach**
- Command injection
- Advanced persistent threat (APT)
- Account hijacking

Correct answer: Data breach

A data breach occurs when data is leaked or stolen, either intentionally or unintentionally. This is not an Advanced Persistent Threat (APT). An APT requires an advanced level of skill from bad actors who usually will be attacking for one nation state against another.

Account hijacking is a step along the way when the bad actor assumed the role that the firewall had to access the database. The whole attack was for the purpose of stealing the data, which is a data breach.

Command injection occurs when a bad actor types a command into a field that is interpreted by the server. This is similar to an SQL injection.

16.

Which of the following is PRIMARILY a concern in multi-cloud environments?

Interoperability

Resiliency

Availability

Performance

Correct answer: Interoperability

Some important cloud considerations have to do with its effects on operations. These include:

- *Availability: The data and applications that an organization hosts in the cloud must be available to provide value to the company. Contracts with cloud providers commonly include service level agreements (SLAs) mandating that the service is available a certain percentage of the time.*
- *Resiliency: Resiliency refers to the ability of a system to weather disruptions. Resiliency in the cloud may include the use of redundancy and load balancing to avoid single points of failure.*
- *Performance: Cloud contracts also often include SLAs regarding performance. This ensures that the cloud-based services can maintain an acceptable level of operations even under heavy load.*
- *Maintenance and Versioning: Maintenance and versioning help to manage the process of changing software and other systems. Updates should only be made via clear, well-defined processes.*
- *Reversibility: Reversibility refers to the ability to recover from a change that went wrong. For example, how difficult it is to restore on-site operations after a transition to an outsourced service (like a cloud provider).*
- *Portability: Different cloud providers have different infrastructures and may do things in different ways. If an organization's cloud environment relies too much on a provider's unique implementation or the provider doesn't offer easy export, the company may be stuck with that provider due to vendor lock-in.*
- *Interoperability: With multi-cloud environments, an organization may have data and services hosted in different providers' environments. In this case, it is important to ensure that these platforms and the applications hosted on them are capable of interoperating.*

- *Outsourcing: Using cloud environments requires handing over control of a portion of an organization's infrastructure to a third party, which introduces operational and security concerns.*

17.

Rogelio is working with the deployment team to deploy 50 new servers as virtual machines (VMs). The servers that he will be deploying will be a combination of different Operating Systems (OS) and Databases (DB). When deploying these images, it is critical to make sure...

That the golden images are always used for each deployment

That the VMs are updated and patched as soon as they are deployed

That the VM images are pulled from a trusted external source

That the golden images are used and then patched as soon as it is deployed

---

Correct answer: That the golden images are always used for each deployment

The golden image is the current and up-to-date image that is ready for deployment into production. If an image needs patching, it should be patched offline and then the new, better version is turned into the new current golden image. Patching servers in deployment is not the best idea. Patching the image offline is the advised path to take.

The golden image should be built within a business, not pulled from an external source, although there are exceptions. It is critical to know the source of the image (IT or security) and to make sure that it is being maintained and patched on a regular basis.

18.

Bai is working on moving the company's critical infrastructure to a public cloud provider. Knowing that she has to ensure that the company is in compliance with the requirements of the European Union's (EU) General Data Protection Regulation (GDPR) country specific laws since the cloud provider is the data processor, at what point should she begin discussions with the cloud provider about this specific protection?

Data Processing Agreement (DPA) negotiation

Establishment of Service Level Agreements (SLA)

Configuration of the Platform as a Service (PaaS) windows servers

At the moment of reversing their cloud status

Correct answer: Data Processing Agreement (DPA) negotiation

Under the EU's GDPR requirements for each country, there is a requirement for a cloud customer to inform the cloud provider that they will be storing personal data (a.k.a. Personally Identifiable Information—PII) on their servers. This is stated in the DPA, which is more generically called a Privacy Level Agreement (PLA). The cloud provider is a processor because they will be storing or holding the data. It is not necessary for the provider to ever use that data to be considered a processor. So, the first point for discussion with the cloud provider regarding the four answer options listed is the DPA negotiation.

The SLAs are part of contract negotiation, but the DPA is specific to the storage of personal data in the cloud, which is the topic of the question. The configuration of the servers and the removal of data from the cloud provider's environment (reversibility) would involve concerns about personal data. The DPA negotiation is a better answer because the question asks at what point should Bai "begin discussions" with the cloud provider.

19.

Damien is working for a real estate company that is working on their plans to move to an online document service that would allow their customers to sign contracts no matter what computer platform they have in their possession. So, interoperability is a critical aspect that they are concerned with. What best describes interoperability?

The ability for two or more systems to exchange information and mutually use that information

The ability for two customers to share the same pool of resources while being isolated from each other

The ability of customers to make changes to their cloud infrastructure with minimal input from the cloud provider

The ease with which resources can be rapidly expanded as needed by a cloud customer

---

Correct answer: The ability for two or more systems to exchange information and mutually use that information

Interoperability is defined in ISO/IEC 17788 as the ability for two or more systems to exchange information and mutually use that information. As a simple example, a Windows machine and a Mac that can exchange a Word document, where both can use it.

The ability for two customers to share the same pool of resources while being isolated from each other is known as multitenancy.

The ability of customers to make changes to their cloud infrastructure with minimal input from the cloud provider is known as on-demand self-service.

The ease with which resources can be rapidly expanded as needed by a cloud customer is called rapid elasticity.

20.

Which of the following describes the cloud's ability to grow over time as demand increases?

Scalability

Elasticity

Agility

Mobility

Correct answer: Scalability

- *Elasticity refers to a system’s ability to grow and shrink on demand.*
- *Scalability refers to its ability to grow as demand increases.*
- *Agility and mobility are not terms used to describe cloud environments.*

21.

Amal is the CIO of Acme Inc. Amal and the information security team are working with the information technology (IT) team to determine if they should move from an on-premises data center into an Infrastructure as a Service (IaaS) virtual data center. Amal wants to determine whether cloud computing is the right solution in this case.

Which technique will BEST help Amal determine if migrating the on-premise data center to the cloud is a good business decision?

Cost-benefit analysis

Proof of concept

Return on investment calculation for the IaaS platform

Business impact analysis

Correct answer: Cost-benefit analysis

Any organization considering moving from an on-premises solution to the cloud should first perform a cost-benefit analysis to ensure that the decision makes sense for the company.

If the cost-benefit is looking good, then the other answer options can be done. Arguably, you need a team of cloud experts to perform a proper cost-benefit. However, the answer says to hire a team and that is probably more than needed before the initial cost-benefit analysis.

If it looks like the cost-benefit is looking good, then use cloud experts to put together a proof of concept trial to ensure that the technology will work properly for the business.

While calculating return on investment (ROI) is useful, calculating the IaaS ROI without considering the data center's costs and benefits (including ROI) is not the best choice.

Business impact analysis (BIA) focuses on identifying the business impact if an asset, system, or process is degraded or lost.

22.

Server and data center redundancy are solutions designed to primarily address which of the following?

Resiliency

Maintenance

Interoperability

Reversibility

Correct answer: Resiliency

Some important cloud considerations have to do with its effects on operations. These include:

- *Availability: The data and applications that an organization hosts in the cloud must be available to provide value to the company. Contracts with cloud providers commonly include service level agreements (SLAs) mandating that the service is available a certain percentage of the time.*
- *Resiliency: Resiliency refers to the ability of a system to weather disruptions. Resiliency in the cloud may include the use of redundancy and load balancing to avoid single points of failure.*
- *Performance: Cloud contracts also often include SLAs regarding performance. This ensures that the cloud-based services can maintain an acceptable level of operations even under heavy load.*
- *Maintenance and Versioning: Maintenance and versioning help to manage the process of changing software and other systems. Updates should only be made via clear, well-defined processes.*
- *Reversibility: Reversibility refers to the ability to recover from a change that went wrong. For example, how difficult it is to restore original operations after a transition to an outsourced service.*
- *Portability: Different cloud providers have different infrastructures and may do things in different ways. If an organization's cloud environment relies too much on a provider's unique implementation or the provider doesn't offer easy export, the company may be stuck with that provider due to vendor lock-in.*
- *Interoperability: With multi-cloud environments, an organization may have data and services hosted in different providers' environments. In this case, it is important to ensure that these platforms and the applications hosted on them are capable of interoperating.*

- *Outsourcing: Using cloud environments requires handing over control of a portion of an organization's infrastructure to a third party, which introduces operational and security concerns.*

23.

Which of the following is MOST relevant to an organization's network of applications and APIs in the cloud?

Service Access

User Access

Privilege Access

Physical Access

Correct answer: Service Access

Key components of an identity and access management (IAM) policy in the cloud include:

- *User Access: User access refers to managing the access and permissions that individual users have within a cloud environment. This can use the cloud provider's IAM system or a federated system that uses the customer's IAM system to manage access to cloud services, systems, and other resources.*
- *Privilege Access: Privileged accounts have more access and control in the cloud, potentially including management of cloud security controls. These can be controlled in the same way as user accounts but should also include stronger access security controls, such as mandatory multi-factor authentication (MFA) and greater monitoring.*
- *Service Access: Service accounts are used by applications that need access to various resources. Cloud environments commonly rely heavily on microservices and APIs, making managing service access essential in the cloud.*

Physical access to cloud servers is the responsibility of the cloud service provider, not the customer.

24.

Which essential characteristic of the cloud says that an organization only pays for what it uses rather than maintaining dedicated servers, operating systems, virtual machines, and so on?

Measured service

On-demand self-service

Broad network access

Multi-tenancy

Correct answer: Measured service

Measured service means that Cloud Service Providers (CSP) bill for resources consumed. With a measured service, everyone pays for the resources they are using.

On-demand self-service means that the user/customer/tenant can go to a web portal, select their service, configure it, and get it up and running without interaction with the CSP.

Broad network access means that as long as the user/customer/tenant has access to the network (the "cloud" is on), they will be able to use that service using standard mechanisms.

Multi-tenancy is a characteristic that exists with all cloud deployment models (public, private, and community). It means that there are multiple users/customers/tenants using the same physical server. The hypervisor has the responsibility of isolating them from each other. In a private cloud, the different users or tenants would be different business units or different projects. A good read is the free ISO standard 17788. Pay particular attention to the definition of multi-tenancy.

25.

Through the International Standard Organization/International Electrotechnical Commisoon (ISO/IEC) 15408-1:2009, what does an EAL2 score tell us about the organization's security practices and results?

It has been structurally tested

It has been functionally tested

It has been methodically tested and checked

It has a formally verified design and has been tested

Correct answer: It has been structurally tested

ISO 15408 is known as the common criteria. It is a testing criteria for security products to ensure fair and even testing when performed in different labs in different countries for similar products.

The possible Evaluation Assurance Level (EAL) scores are as follows:

- *EAL1 - Functionally tested*
- ***EAL2 - Structurally tested***
- *EAL3 - Methodically tested and checked*
- *EAL4- Methodically designed, tested, and reviewed*
- *EAL5 - Semi-formally designed and tested*
- *EAL6 - Semi-formally verified design and tested*
- *EAL7 - Formally verified design and tested*

Although this is a very simple question, it is worth noting that this is information that could be useful to know for the test.

26.

Under which of the following cloud service models does the cloud provider control the LARGEST portion of the infrastructure stack?

SaaS

PaaS

IaaS

FaaS

Correct answer: SaaS

Cloud services are typically provided under three main service models:

- *Software as a Service (SaaS): Under the SaaS model, the cloud provider offers the customer access to a complete application developed by the cloud provider. Webmail services like Google Workspace and Microsoft 365 are examples of SaaS offerings.*
- *Platform as a Service (PaaS): In a PaaS model, the cloud provider offers the customer a managed environment where they can build and deploy applications. The cloud provider manages compute, data storage, and other services for the application.*
- *Infrastructure as a Service (IaaS): In IaaS, the cloud provider offers an environment where the customer has access to various infrastructure building blocks. AWS, which allows customers to deploy virtual machines (VMs) or use block data storage in the cloud, is an example of an IaaS platform.*

Function as a Service (FaaS) is a form of PaaS in which the customer creates individual functions that can run in the cloud. Examples include AWS Lambda, Microsoft Azure Functions, and Google Cloud Functions.

27.

Which of the following refers to a cloud customer's ability to grow or shrink their cloud footprint on demand?

Elasticity

Scalability

Agility

Mobility

Correct answer: Elasticity

- *Elasticity refers to a system's ability to grow and shrink on demand.*
- *Scalability refers to its ability to grow as demand increases.*
- *Agility and mobility are not terms used to describe cloud environments.*

28.

Which cloud characteristic is discussed when the Central Processing Unit (CPU), memory, network capacity, and other things are allocated to customer virtual machines as they are needed?

Resource pooling

On-demand self-service

Interoperability

Broad network access

Correct answer: Resource pooling

When the resources, such as CPU, memory, and network, are gathered into a pool and allocated to running virtual machines as needed, resource pooling is being discussed.

On-demand self-service is when the cloud provider (private, public, or community) provides a web interface to navigate offerings and purchase them, such as AWS.amazon.com.

Interoperability is the ability for two different systems to be able to share a piece of data and use it, such as a word doc being created on a Mac and sent to a Windows device and be readable.

Broad network access is the requirement of the cloud, which means that network access must be there, and when it is there, the customer can use the cloud.

29.

A cloud provider has assembled all the cloud resources from routers to servers and switches, as well as the central processing unit (CPU), random access memory (RAM), and storage within the servers. Then, they made them available for allocation to their customers.

Which term BEST describes this process?

Resource pooling

Reversibility

Data portability

On-demand self-service

Correct answer: Resource pooling

Cloud providers may choose to do resource pooling, which is the process of aggregating all the cloud resources together and allocating them to their cloud customers. There is pooling of physical equipment into the data center. Then there is a pool of resources within a server that are allocated to running virtual machines. That is the CPU, the RAM, and the available network bandwidth.

Multi-tenancy occurs when a service provider gives multiple users (tenants) an allocation of shared resources. Resource pooling enables multitenancy, but the act of a service provider pooling their resources is not multitenancy.

Portability is the ability to move data from one provider to another without having to reenter the data.

On-demand self-service is the ability for the customer/tenant to use a portal to purchase and provision cloud resources without having much, if any, interaction with the cloud provider.

30.

Which of the following is a standard that defines the requirements for cryptographic modules?

FIPS 140-2

Common Criteria

ISO 27002

ISO 27017

Correct answer: FIPS 140-2

Cloud providers' systems may be subject to certification against standards that address a specific component, such as a cryptographic module. Examples of these system/subsystem product certifications include:

- *Common Criteria: Common Criteria (CC) are guidelines for comparing various security systems. A protection profile describes the security requirements of systems being compared, and the evaluation assurance level (EAL) describes the level of testing performed on the system, ranging from 1 (lowest) to 7 (highest).*
- *FIPS 140-2: Federal Information Processing Standard (FIPS) 140-2 is a US government standard for cryptographic modules. FIPS compliance is necessary for organizations that want to work with the US government and mandates the use of secure cryptographic algorithms like AES.*

ISO 27017 is an ISO (International Organization for Standardization) standard focused on the implementation of security controls from ISO 27002 (another ISO standard that provides specific security controls) in cloud environments.

31.

Rhonda works for a retail clothing store in the United States as their information security manager. She has been working with the legal department to ensure they comply with all required laws and contracts.

Which of the following MOST LIKELY applies?

Their payment card companies must follow the Payment Card Industry - Data Security Standard (PCI-DSS)

They must protect employee medical data that they store, according to HIPAA

They must comply with the United States law referred to as the PCI-DSS

They must comply with the European Union's contractual requirement of GDPR

Correct answer: Their payment card companies must follow the Payment Card Industry - Data Security Standard (PCI-DSS)

The PCI-DSS is a contractual requirement that applies to companies that accept and process payment cards. As a retail store, this definitely applies to the data that they have in their possession.

As a retail clothing store, it is unlikely that they will have health data from their employees. Since credit cards are a definite piece of data that they have, PCI-DSS is a better answer.

PCI-DSS is a contractual requirement, not a law, nor is it US-specific.

The question is not specific as to where the store is, so they may be within the EU. If they are in the EU, the GDPR would apply. However, GDPR is a law, not a contract.

32.

An information security manager is concerned about the security of portable devices in the organization that have been given access to corporate resources. What can this information security manager implement to manage and maintain the devices?

MDM

SIEM

BYOD

VPN

Correct answer: MDM

Mobile device management (MDM) is the term used to describe the management and maintenance of mobile devices (e.g., tablets and mobile phones) that have access to corporate resources. Usually, MDM software will be installed on the devices so that the IT staff can manage the devices remotely in the case of a lost or stolen device.

MDM software usually has the following:

1. *Symmetric encryption technology for the drive on the mobile device*
2. *Remote control to be able to disable or even "brick" the device if it is lost or stolen*
3. *Remote control to be able to delete files in the event the phone is lost or stolen*

Bring your own device (BYOD) is a model where employees use their own devices for work-related activities. BYOD environments are a common example of a use case for MDM.

Using a security information and event management (SIEM) tool is good practice but does not directly enable device management.

A virtual private network (VPN) can reduce the risk of network-related incidents but does not directly enable device management. An MDM could enforce a VPN on devices that need access to sensitive resources.

33.

Which of the following tasks is typically easier for operators of private cloud environments?

Scheduling maintenance downtime

Scaling infrastructure

Onboarding new tenants

Encrypting data

Correct answer: Scheduling maintenance downtime

Private cloud deployments reduce challenges related to multi-tenancy. For example, scheduling maintenance downtime with one organization is typically simpler than scheduling downtime when multiple organizations are involved.

Private clouds are dedicated to a single organization, so onboarding new tenants is incorrect.

Encrypting data and scaling infrastructure are not typically considered easier for a private cloud operator.

34.

Lightweight operating systems like Ubuntu Core and the Zephyr real-time operating system are MOST LIKELY to be used in which applications?

Internet of Things

Physical servers

Virtual machines

Blockchain

Correct answer: Internet of Things

The Internet of Things (IoT) refers to non-traditional devices (e.g., lamps, refrigerators, or machines in a manufacturing environment) having access to the internet to perform various processes. IoT devices typically run lightweight operating systems due to limited resources on smart devices.

Virtual machines are constructed within the cloud through the use of hypervisors on top of servers. Virtual machines can run many different operating systems and using lightweight operating systems like Ubuntu Core and the Zephyr real-time operating system are not particularly common for VMs. Similarly, physical servers can run a wide variety of operating systems, and "server" operating systems such as Server 2019 or Ubuntu 22.04 LTS are more typically associated with servers.

Containers hold applications in a lighter way than hypervisors.

Blockchain is a technology that creates an immutable (i.e., unchangeable) record. It is used in things like cryptocurrency. It is possible to sell anything, though, and use the blockchain as a permanent record of the transaction.

35.

Which of the following is a major difference between public and private cloud environments?

Multitenancy

On-Demand Self-Service

Broad Network Access

Resource Pooling

Correct answer: Multitenancy

The six common characteristics of cloud computing include:

- *Broad Network Access: Cloud services are widely available over the network, whether using web browsers, secure shell (SSH), or other protocols.*
- *On-Demand Self-Service: Cloud customers can redesign their cloud infrastructure at need, leasing additional storage or processing power or specialized components and gaining access to them on-demand.*
- *Resource Pooling: Cloud customers lease resources from a shared pool maintained by the cloud provider at need. This enables the cloud provider to take advantage of economies of scale by spreading infrastructure costs over multiple cloud customers.*
- *Rapid Elasticity and Scalability: Cloud customers can expand or contract their cloud footprint at need, much faster than would be possible if they were using physical infrastructure.*
- *Measured or Metered Service: Cloud providers measure their customers' usage of the cloud and bill them for the resources that they use.*
- *Multitenancy: Public cloud environments are multitenant, meaning that multiple different cloud customers share the same underlying infrastructure. Private cloud environments are single-tenant environments used by a single organization.*

36.

Which of the following emerging technologies REDUCES the amount of computation performed on cloud servers?

Edge Computing

Artificial Intelligence

Blockchain

TEE

Correct answer: Edge Computing

Cloud computing is closely related to many emerging technologies. Some examples include:

- *Machine Learning and Artificial Intelligence (ML/AI): Machine learning is a subset of AI and includes algorithms that are designed to learn from data and build models to identify trends, perform classifications, and other tasks. Cloud computing is linked to the rise of ML/AI because it provides the computing power needed to train the models used by ML/AI and operate these technologies at scale.*
- *Blockchain: Blockchain technology creates an immutable digital ledger in a decentralized fashion. It is used to support cryptocurrencies, track ownership of assets, and implement various other functions without relying on a centralized authority or single point of failure. Cloud computing is related to blockchain because many of the nodes used to maintain and operate blockchain networks run on cloud computing platforms.*
- *Internet of Things (IoT): IoT systems include smart devices that can perform data collection or interact with their environments. These devices often have poor security and rely on cloud-based servers to process collected data and issue commands back to the IoT systems (which have limited computational power, etc.).*
- *Edge and Fog Computing: Edge and fog computing move computations from centralized servers to devices at the network edge, enabling faster responses and less usage of bandwidth and computational power by cloud servers. Edge computing performs computing on IoT devices, while fog computing uses gateways at the edge to collect data from these devices and perform computation there.*

- *Confidential computing: With confidential computing, cryptography is used to protect data in the cloud. A trusted execution environment (TEE) enables data decryption only for specific authorized access attempts.*

37.

A large consulting firm has a hybrid cloud environment. They have a private cloud that they manage on their premises, and they use a large public cloud provider for some of their Platform and Software as a Service (PaaS and SaaS) needs. Their security operations center (SOC) has been processing a few high-priority indications of compromise (IoC) that appear to point to a live incident.

For their response, what should they do?

Observe, Orient, Decide, Act

Reconnaissance, Execution, Evasion, Collection

Reconnaissance, Delivery, Exploitation

Sense, Categorize, Respond

Correct answer: Observe, Orient, Decide, Act

The OODA loop is Observe, Orient, Decide, and Act. This is a common incident response concept. The OODA loop is iterative: after completing one cycle, individuals continuously loop back to the beginning to gather new information, reassess the situation, and make further decisions and actions. The loop emphasizes the importance of speed, adaptability, and learning from feedback to maintain a competitive advantage and effectively respond to dynamic and uncertain situations.

"Sense, categorize, and respond" is taken from the Cynefin Framework and is used for clear situations with fixed constraints. Incident response is typically not clear enough at the onset to fit into the "clear" category of the Cynefin Framework.

Kill chains are the path that bad actors take in their attacks. They are good to be familiar with. In their entirety, they are as follows:

- *The Lockheed-Martin Kill Chain is a comprehensive cybersecurity strategy that helps organizations identify and prevent advanced cyber attacks at various stages of the attack process. The concept is based on the idea of a chain, where each stage represents a link in the chain that can be broken or disrupted, effectively stopping the cyber attack from being successful. The stages are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives.*
- *The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, according to MITRE's website, "is a comprehensive knowledge base that describes the various Tactics, Techniques, and Procedures (TTPs) used by adversaries during cyberattacks. It provides a*

structured and standardized way of understanding and categorizing the different stages of an attack. One of the frameworks within MITRE ATT&CK is the "ATT&CK Kill Chain." The kill chain steps are Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact."

38.

A company offers integrated security services for a cloud environment. Which of the following BEST describes their role?

Cloud Service Partner

Cloud Service Provider

Cloud Service Broker

Cloud Customer

Correct answer: Cloud Service Partner

Some of the important roles and responsibilities in cloud computing include:

- *Cloud Service Provider: The cloud service provider offers cloud services to a third party. They are responsible for operating their infrastructure and meeting service level agreements (SLAs).*
- *Cloud Customer: The cloud customer uses cloud services. They are responsible for the portion of the cloud infrastructure stack under their control.*
- *Cloud Service Partners: Cloud service partners are distinct from the cloud service provider but offer a related service. For example, a cloud service partner may offer add-on security services to secure an organization's cloud infrastructure.*
- *Cloud Service Brokers: A cloud service broker may combine services from several different cloud providers and customize them into packages that meet a customer's needs and integrate with their environment.*
- *Regulators: Regulators ensure that organizations — and their cloud infrastructures — are compliant with applicable laws and regulations. The global nature of the cloud can make regulatory and jurisdictional issues more complex.*

39.

Acme Inc. would like to move its environment from one cloud provider to another. However, the cloud provider implemented techniques that have made it very difficult to move systems to a new provider.

What is this an example of, and how can Acme Inc. reduce the risk of the same thing happening with another vendor?

This is an example of vendor lock-in. Negotiating better contract terms could prevent similar incidents.

This is an example of strong interoperability. Using stronger encryption could prevent similar incidents.

This is an example of portability. Negotiating better contract terms could prevent similar incidents.

This is an example of vendor lock-out. Negotiating better contract terms could prevent similar incidents.

Correct answer: This is an example of vendor lock-in. Negotiating better contract terms could prevent similar incidents.

Vendor lock-in is when a cloud customer is stuck using one cloud provider for one reason or another. Vendor lock-in can occur when the cloud provider has implemented technologies that make it difficult for the customer to move their data without hassle to another provider (e.g., when Apple created iTunes and imported music as .aac rather than .mpeg). Customers can reduce the risk of vendor lock-in by negotiating favorable contract terms for data portability, ensuring data is stored in raw formats, and confirming no major constraints are preventing them from leaving a vendor.

Interoperability means that data created on one type of system (e.g., Microsoft 365 on a Mac) can be read on a different system (e.g., Microsoft 365 on a Windows machine).

Portability is when data can be moved from one cloud provider to another without having to be recreated.

Vendor lock-out occurs when a vendor goes out of business, is acquired, or otherwise ceases to operate and their clients lose access to data or services. Vendor lock-out is not described in the question because there is no indication the vendor ceased operations.

Strong encryption would not directly address a vendor lock-in problem.

40.

Acme Inc. wants to use a cloud service model for its applications. Acme Inc. has requirements to reduce maintenance costs and limit its capital expenditures. There is no single cloud service provider that meets all of their application-level requirements.

Which of the following cloud models is the BEST choice for Acme Inc. to optimize its cloud environment for the various applications and data being hosted there?

Multi-Cloud

Private Cloud

Community Cloud

Public Cloud

Correct answer: Multi-Cloud

Cloud services are available under a few different deployment models, including:

- *Private Cloud: In private clouds, the cloud customer builds their own cloud in-house or has a provider do so for them. Private clouds have dedicated servers, making them more secure but also more expensive.*
- *Public Cloud: Public clouds are multi-tenant environments where multiple cloud customers share the same infrastructure managed by a third-party provider.*
- *Hybrid Cloud: Hybrid cloud deployments mix both public and private cloud infrastructure. This allows data and applications to be hosted on the cloud that makes the most sense for them.*
- *Multi-Cloud: Multi-cloud environments use cloud services from multiple different cloud providers. This enables customers to take advantage of price differences or optimizations offered by different providers.*
- *Community Cloud: A community cloud is essentially a private cloud used by a group of related organizations rather than a single organization. It could be operated by that group or a third party, such as FedRAMP-compliant cloud environments operated by cloud service providers.*

Since the question emphasizes that there is no single cloud service provider that meets all of their requirements, multi-cloud is a better answer than public cloud. Acme Inc.'s desire to reduce capital expenditures makes private cloud a less viable option.

41.

Dana is developing a cloud migration business case to propose to the board of directors.

While weighing the different options for cloud deployment, Dana and her team are exploring public, private, and hybrid clouds. They currently have a moderate-sized data center that includes servers running many traditional operating systems.

Which of the following will Dana's team likely recognize as a benefit of using a public cloud deployment?

Inexpensive

Full ownership of data

Control over systems

Security

Correct answer: Inexpensive

A public cloud is often considered the least expensive cloud deployment option. Public clouds are available to the general public, and customers only pay for the services that they use. All expenses ranging from the licensing, hardware, bandwidth, and operational costs are handled by the provider.

Public clouds do not offer full control over the systems in the way that private clouds do. If they move to an Infrastructure as a Service (IaaS), they will have control over all the virtual systems, including routers, switches, servers, and security appliances. However, the question does not say they are moving to IaaS, but even if they do, they do not have control over the physical systems.

They always, or should always, have full ownership of the data, so that is not a benefit of public versus private or hybrid.

While many variables determine if a cloud environment is secure, private clouds are typically viewed as more secure than public clouds due to the increased isolation and control.

42.

Acme Inc.'s cybersecurity team just declared a network breach as a cybersecurity incident and assigned Vaeda as the incident manager to coordinate further actions. What phase of the incident response lifecycle are Vaeda and the team in?

Detection and Analysis

Recovery

Governance

Containment

Correct answer: Detection and Analysis

The incident manager is in the second phase, detection and analysis.

The Cloud Security Alliance (CSA) guidance 4.0 document (watch for v5 as of May 2023) breaks down the phases in the following manner:

***Preparation**: Establishing an incident response capability so that the organization is ready to respond to incidents.*

- *Process to handle the incidents*
- *Handler communications and facilities*
- *Incident analysis hardware and software*
- *Internal documentation (port lists, asset lists, network diagrams, current baselines of network traffic)*
- *Identifying training*
- *Evaluating infrastructure by proactive scanning and network monitoring, vulnerability assessments, and performing risk assessments*
- *Subscribing to third-party threat intelligence services*

***Detection and Analysis:** This is really when managing a real risk begins. Preparation is getting ready. Detection is when it has happened, and we discover it in someway. The analysis is often stated as triage. It is necessary to determine what is happening and what will be handled by the team first.*

- *Alerts (endpoint protection, network security monitoring, host monitoring, account creation, privilege escalation, other indicators of compromise, SIEM, security analytics for baseline and anomaly detection, and user behavior analytics)*
- *Validate alerts (reducing false positives) and escalation*
- *Estimate the scope of the incident*

- *Assign an incident manager who will coordinate further actions*
- *Designate a person who will communicate the incident containment and recovery status to senior management*
- *Build a timeline of the attack*
- *Determine the extent of the potential data loss*
- *Notification and coordination activities*

Containment, Eradication, and Recovery: *We often want to start the containment as soon as we detect it. We need to analyze it to be able to determine the containment step. This could occur minutes, hours, or days after the incident happens. Once the attack is contained, it is necessary to clean and remove any remnants of the attack (e.g., Is there a virus on a system that needs to be removed?). Otherwise, it is necessary to return our environments to a normal condition. It could be that we also need to change a control, alter a configuration, add a new control somewhere, etc. to ensure this does not happen again.*

- *Containment: Taking systems offline. Considerations for data loss versus service availability. Ensuring systems don't destroy themselves upon detection*
- *Eradication and Recovery: Clean up compromised devices and restore systems to normal operation. Confirm systems are functioning properly. Deploy controls to prevent similar incidents*
- *Documenting the incident and gathering evidence (chain of custody)*

Post-mortem: *Now that things are back to normal, what could have been handled differently that would have made things better? This is a meeting to work together to get better. It is not a finger-pointing exercise. Own what we did right and what we did wrong.*

- *What could have been done better? Could the attack have been detected sooner? What additional data would have been helpful to isolate the attack faster?*
- *Does the IR process need to change? If so, how?*

Governance is the oversight provided by the Board of Directors and the C-suite, encompassing corporate governance, security governance, and data governance.

Privacy is a critical topic. There are so many regulations being created or updated to force companies to take the act of protecting their customers' and employees' personal information.

Neither governance nor privacy is directly part of the incident response. They are not phases. Depending on how you look at things, they are connected but not directly.

43.

Which of the following cloud design principles can reduce the risk of vendor lock-in?

- **Portability**
- Interoperability
- Reversibility
- Multi-tenancy

Correct answer: Portability

The ability to move data between multiple cloud providers is known as cloud data portability. Cloud application portability refers, instead, to the ability to move an application between cloud providers. If applications and data have high portability, the risk of vendor lock-in is typically low.

Multi-tenancy describes a cloud provider housing multiple customers and/or applications within one server.

Interoperability is the ability of two different systems to exchange and use a piece of data, such as one user creating a Microsoft Word document on a Mac and then another user opening and using that document on a Microsoft Windows machine.

Reversibility is the ability to retrieve data from a cloud provider upon termination of the contract, as well as having the data be removed securely from the cloud provider's systems.

These terms are defined in ISO 17788, which is the ISO version of NIST 800-145.

44.

Nica has been hired by a law firm to manage their information security department. It has been determined that they will be closing down their on-premises data center after they complete their move to the cloud. This law firm handles legal affairs for a hospital located in the USA. Which laws are most relevant to this client?

The California Consumer Privacy Act (CCPA) and the Health Information Portability and Accountability Act (HIPAA)

The Health Information Portability and Accountability Act (HIPAA) and the Personal Information Protection and Electronic Act (PIPEDA)

The Personal Information Protection and Electronic Act (PIPEDA) and Sarbanes Oxley (SOX)

Sarbanes Oxley (SOX) and the Gramm Leach and Bliley Act (GLBA)

Correct answer: The California Consumer Privacy Act (CCPA) and the Health Information Portability and Accountability Act (HIPAA)

CCPA and HIPAA are the best match to a hospital in the US. The assumption is that the hospital is in California, so it is unlikely to be the other combination of laws. PIPEDA is from Canada.

SOX relates to US businesses, but it is related to financial integrity. GLBA is from the US as well, but it is about protecting the personal information of customers from financial services companies. A hospital could be a financial services company if it sets up payment plans for its customers. It is arguable that SOX does apply to a hospital, but HIPAA absolutely matches the hospital.

45.

Which of the following solutions can be difficult to secure because certain security solutions can't be deployed without an underlying OS?

Serverless

LXC

Type 2 hypervisor

Type 1 hypervisor

Correct answer: Serverless

Some important security considerations related to virtualization include:

- *Hypervisor Security: The primary virtualization security concern is isolation or ensuring that different VMs can't affect each other or read each other's data. VM escape attacks occur when a malicious VM exploits a vulnerability in the hypervisor or virtualization platform to accomplish this. Type 1 hypervisors are installed directly on server hardware, while type 2 hypervisors are installed on a host operating system (e.g., Windows 11 or Ubuntu 22.04).*
- *Container Security: Containers are self-contained packages that include an application and all of the dependencies that it needs to run. Containers improve portability but have security concerns around poor access control and container misconfigurations. Linux containers (LXC) is one example of a containerization technology.*
- *Ephemeral Computing: Ephemeral computing is a major benefit of virtualization, where resources can be spun up and destroyed at need. This enables greater agility and reduces the risk that sensitive data or resources will be vulnerable to attack when not in use. However, these systems can be difficult to monitor and secure since they only exist briefly when they are needed, so their security depends on correctly configuring them.*
- *Serverless Technology: Serverless applications are deployed in environments managed by the cloud service provider. Outsourcing server management can make serverless systems more secure, but it also means that organizations can't deploy traditional security solutions that require an underlying OS to operate.*

46.

Leonidas has been working through the process of assessing and evaluating potential cloud providers to host their needs within the Platform as a Service (PaaS) cloud model. One of the critical aspects that he has been trying to determine is if they will be able to remove their data from the cloud provider in the future should they determine that the cloud is not the right solution for them or if they need to change service providers.

What term matches their concern of removing their data from the cloud provider?

- **Reversibility**
- Availability
- Portability
- Interoperability

Correct answer: Reversibility

Reversibility is the ability to retrieve their data and artifacts and ensure the complete removal of that data and artifacts from the cloud provider.

Portability is the ability to move all data from one cloud provider to another without having to reenter that data.

Interoperability is the ability of two different systems to share and use a piece of data.

Availability means that the data and systems are there and usable when the user requires access.

47.

Giovanni is working with the legal department on a cloud contract with a Managed Service Provider (MSP). They are working on the language of the service level agreement (SLA) for their performance concerns. They require an uptime of 99.9995%.

What performance concern are they addressing?

- **Availability**
- Bandwidth
- Resource utilization
- Memory

Correct answer: Availability

With an uptime requirement of 99.9995%, they are addressing availability. That availability, or lack thereof, could be from bandwidth issues, CPU issues, memory issues, or others.

Availability is the better answer because it includes the other three. This is how the $(ISC)^2$ does "all of the above" type of questions.

48.

Dawson is an information security manager for a Fortune 500 company. He and his team have been working on revising their data governance strategy and the resulting policy. They have decided that they will need to deploy more Data Loss Prevention systems to inspect data on their file systems. They have been experiencing small breaches of data, and they are looking for the source.

What phase of the cloud data lifecycle are they in?

Store

Share

Use

Archive

Correct answer: Store

Since the data is sitting on a file server, the data is in storage. Archival is a type of storage, but there is nothing in the question to lead us to archive. So, store fits the environment of the question better.

They might be losing control of data when it is shared, but DLP to inspect the file systems is not data in transit, it is data at rest. Traditionally, DLP systems only helped us when the data was in transit, but that is no longer the case.

The data breach may be caused by some action a user is taking when they are in the use phase, but again, the DLP system is inspecting the file system, which is data at rest.

49.

A corporation has submitted their product, a Hardware Security Module (HSM), for testing. They need to prove to their customers that it is going to be able to protect itself from physical tampering. The tester has proven that their product will detect tampering attacks and overwrite the stored data with zeros. What have they achieved?

FIPS 140-3 Level 3

Common Criteria Level 4

Common Criteria Level 3

FIPS 140-3 Level 2

Correct answer: FIPS 140-3 Level 3

The National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 or 140-3 is a criterion for the physical security of cryptographic modules. A level 2 certification means that there will be evidence of tampering such as a cut piece of tape. Level 3 products must be able to detect the tampering and respond by zeroizing the data, including the crypto keys that it stores.

Common criteria is International Standards Organization (ISO) 15408. Level 3 is methodically designed and tested. Level 4 is methodically designed, tested, and reviewed.

50.

Customers often require audits of cloud solutions, including public cloud platforms. Which of the following parties typically audits a cloud service provider and performs assessments that customers can use?

An independent third party

The customer

The cloud service provider

OWASP

Correct answer: An independent third party

Auditability is the process of gathering and making available the evidence necessary to demonstrate the operation and use of the cloud. Customers are often interested in audits and assessments of their cloud platforms, but a cloud service provider (CSP) rarely allows a customer to perform an audit on their controls. However, it is more common for CSPs to allow third-party assessments that audit security controls. These assessments may require a nondisclosure agreement (NDA).

The Open Worldwide Application Security Project (OWASP) is a community focused on web application security that provides a variety of free resources.

51.

Acme Inc. has been looking for a technology that would aid their business in its decision-making processes. They are trying to learn from all the data that they have so that they can make better decisions. In particular, they are trying to figure out how to reduce the costs of their manufacturing processes.

Which technology would be BEST for providing specific recommendations for cost reductions?

Prescriptive analytics

Predictive analytics

Descriptive analytics

Blockchain

Correct answer: Prescriptive analytics

Prescriptive analytics uses mathematical models and optimization techniques to recommend actions or decisions based on a given set of constraints, objectives, and possible outcomes (such as how to gain a competitive advantage, reduce costs, and improve performance).

Predictive analytics focuses on analyzing historical data and predicting future outcomes.

Descriptive analytics analyzes information and provides details regarding that data.

Blockchain uses cryptography to enable nonrepudiation and anonymous transactions.

52.

Acme Inc. wants to ensure that the sensitive data they have stored on a cloud platform is securely sanitized. Which of the following media sanitization techniques is BEST for this scenario?

Cryptographic erasure

Overwriting

Physical destruction

Degaussing

Correct answer: Cryptographic erasure

When disposing of potentially sensitive data, organizations can use a few different data and media sanitization techniques, including:

- *Overwriting involves writing random data or all 0's or all 1's over sensitive data. This may be less effective in the cloud if the customer can guarantee access to certain regions of memory on the underlying server.*
- *Cryptographic erasure involves destroying the encryption keys used to protect sensitive data. This can easily be accomplished in the cloud by deleting keys from the key management system (KMS).*

Physical destruction of media and degaussing are not options in the cloud because the customer lacks access to and control over the physical media used to store data.

53.

Ariel is a cloud administrator configuring a Platform as a Service (PaaS) server-based deployment on a public cloud provider. She needs to know the agreed-upon central processing unit (CPU) speed and bandwidth to configure the server.

Where could Ariel find this information?

SLA

MoU

MSA

PLA

Correct answer: SLA

A service level agreement (SLA) is an agreement that provides specific requirements that must be met by the cloud provider for contractual satisfaction between the cloud customer and the cloud provider. The requirements are usually measurable, such as bandwidth and CPU performance.

A master service agreement (MSA) is the agreement between the cloud service provider (CSP) and the cloud customer (CC). This defines their role in the relationship.

A privacy level agreement (PLA) is a generic form of the data processing agreement (DPA) for GDPR or the business associate agreement (BAA) for HIPAA. This tells the cloud provider the type of personal data that is being stored and processed on their systems and the level of protection the CC expects from the CSP.

A memorandum of understanding (MoU) defines the broad agreement that the two parties, CSP and CC, have agreed to and is not as common with cloud services.

54.

A cloud service provider (CSP) wants to do business with the United States government. Which of the following standards will they be audited against to validate they can sell their services to the United States government?

FedRAMP

FIPS 140

PCI DSS

ISO/IEC 27017

Correct answer: FedRAMP

Cloud service providers may have their environments verified against certain standards, including:

- *ISO/IEC 27017 and 27018: The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) publishes various standards, including those describing security best practices. ISO 27017 and ISO 27018 describe how the information security management systems and related security controls described in ISO 27001 and 27002 should be implemented in cloud environments and how PII should be protected in the cloud.*
- *PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) was developed by major credit card brands to protect the personal data of payment card users. This includes securing and maintaining compliance with the underlying infrastructure when using cloud environments.*
- *Government Standards: FedRAMP-compliant offerings and UK G-Cloud are cloud services designed to meet the requirements of the US and UK governments for computing resources. FedRAMP is a standard used for auditing potential CSPs for the United States government.*

FIPS 140 is a standard for cryptographic modules. FIPS 140 compliance does not directly enable a CSP to sell to the United States government.

55.

In which of the following cloud deployment models is the cloud provider responsible for the operating systems and hosting environment, while the customer is responsible for deploying their applications within the provided platform infrastructure?

Platform as a Service (PaaS)

Software as a Service (SaaS)

Infrastructure as a Service (IaaS)

Communication as a Service (CaaS)

Correct answer: Platform as a Service (PaaS)

In a PaaS cloud deployment model, the cloud provider manages and maintains the operating system and hosting environment, while the customer is only responsible for deploying their applications within the given platform.

In SoaS, the customer is responsible for their data, but the provider is responsible for the software/application, Operating Systems (OS), and everything else within and below there.

In IaaS, the customer is responsible for the OSs that they bring to the cloud, which includes their servers, virtual desktops, databases, routers, firewalls, switches, etc. and everything above the OS. The provider is responsible for the hypervisor and everything below that.

CaaS is probably a SaaS deployment. So, the customer is responsible for their data (calls, chats, recordings, etc.), and the provider is responsible for the application and everything below.

56.

A corporation has hired Adit as the information security manager responsible for Business Continuity Management (BCM) throughout the business. The current plan that Adit and his team are working on is the critical plan that the incident responders will utilize if there is an event such as a fire or earthquake that affects the data center. The assumption that they are working on is that the facility itself will be destroyed, and they will need to move operations to a different location, at least, temporarily.

Which type of document would this be?

- **Disaster Recovery Plan (DRP)**
- Business Continuity Plan (BCP)
- Incident Response Plan (IRP)
- Acceptable Use Policy (AUP)

Correct answer: Disaster Recovery Plan (DRP)

The US NIST defines DRPs as "a written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities." The DRP is most commonly considered a sub part of business continuity plans. The BCP is defined by NIST as "the documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption." Because the scenario is about the physical destruction of the data center facility and its hardware and software, DRP is the more specific plan.

It is worth noting that this is a debatable take on BCP versus DRP. However, this seems to be the slightly more prevalent one that (ISC)2 seems to agree with.

IRPs are defined by NIST as "the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attack against an organization's information systems(s)."

The AUP informs users of the acceptable uses of resources such as their phones, computers, internet, and data.

57.

A university is looking to make its environment as green as possible. They want to move to solar and wind power to generate enough power for the entire university, including the student dormitories. They have installed smart thermostats throughout the classroom buildings. They have the ability to monitor the current temperature, both inside the classrooms and outside the building. This way, they can individually change based on the needs of the building.

What can enhance this Internet of Things capability?

Edge computing

Fog computing

Internet of Things

Cloud computing

Correct answer: Edge computing

Edge computing is the idea of moving the processing to the logical edge of the network as close to the user and their systems as possible. This manages bandwidth, enhances privacy controls, and if the internet is not accessible, they can continue to manage the temperature locally.

Fog computing is a term that Cisco created that is gaining traction. Fog computing moves the processing of data to a local fog node or IoT gateway.

Cloud computing is what this entire course and certification is about. In domain 1, the focus is understanding that the cloud, especially a public cloud, is using servers and services located in a data center somewhere, hopefully not too far away, but then again, it can be for redundancy purposes.

The Internet of Things is considered by some to just be the connecting of things such as manufacturing equipment to the internet. Others consider it to be anything connected to the internet. Neither is right. It is good to know both to be able to sort out questions.

58.

Which of the following blockchain types requires permission to join but can be open and utilized by a group of different organizations working together?

Consortium

Private

Public

Permissioned

Correct answer: Consortium

Consortium blockchains are a hybrid of public and private blockchains. They are operated by a consortium or a group of organizations that have a shared interest in a particular industry or use case. Consortium blockchains provide a controlled and permissioned environment while still allowing multiple entities to participate in the consensus and decision-making process.

Public blockchains, such as Bitcoin and Ethereum, are open to anyone and allow anyone to participate in the network, verify transactions, and create new blocks. They are decentralized and provide a high level of transparency and security. Public blockchains use consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), to validate transactions and secure the network.

Private blockchains are restricted to a specific group of participants who are granted access and permission to the network. They are typically used within organizations or consortia where participants trust each other and require more control over the network. Private blockchains offer higher transaction speeds and privacy but sacrifice decentralization compared to public blockchains.

Permissioned blockchains require users to have permission to join and participate in the network. They are typically used in enterprise settings where access control and governance are critical. Permissioned blockchains offer faster transaction speeds and are more scalable than public blockchains, but they sacrifice some decentralization and censorship resistance.

59.

An administrator is moving an application from their current cloud provider to a new cloud provider. Which of the following gives them the ability to do this?

Portability

Interoperability

Rapid elasticity

Multi-tenancy

Correct answer: Portability

The ability to move an application between multiple cloud providers is known as cloud portability. To port is to move without having to recreate or reenter the data.

Interoperability is when data can be used by two different systems. For example, a PDF created on a Mac that can be read on a Windows-based system.

Rapid elasticity refers to the ability to quickly (or rapidly) expand and contract to match the needs of the user/application/system. The resources such as CPU, memory, or storage can be increased as needed by the users and decreased when they are no longer needed.

Multi tenancy is always present in cloud servers. The tenants are different customers within the public cloud. In a private cloud, the tenants are different departments or projects. The hypervisor has the responsibility of isolating tenants from each other.

60.

Which of the following statements about public vs. private cloud environments is FALSE?

Public cloud environments are typically more customizable than private cloud environments

Public cloud environments typically have lower upfront costs than private cloud environments

Public cloud environments have a higher risk of service removal than private cloud environments

Public cloud environments are typically lower maintenance than private cloud environments

---

Correct answer: Public cloud environments are typically more customizable than private cloud environments

Public cloud environments are accessible by anyone with an internet connection. Typically, public cloud resources are provided using a subscription model. The vendor is responsible for infrastructure and maintenance related to a public cloud platform. Because users do not control the public cloud, there is a risk of service removal that does not exist with private cloud solutions.

Private cloud environments are dedicated to a single organization. Typically, private cloud environments offer more control and security than public but come with more maintenance, upfront costs, and deployment complexity. Because users have more control over private cloud environments, they are typically more customizable than public cloud environments.

61.

The information security manager is working with the cloud deployment team as they prepare to move their data center to the cloud. An important part of their plan is how they are going to get out of the cloud. They would like to reduce the risk of vendor lock-in. What cloud shared consideration should the administrator be looking for?

Reversibility

Interoperability

Portability

Availability

Correct answer: Reversibility

Reversibility is defined in ISO/IEC 17788 as the "process for cloud service customers to retrieve their cloud service customer data and application artifacts and for the cloud service provider to delete all cloud service customer data as well as contractually specified cloud service derived data after an agreed period." Based on this definition, reversibility is the best fit for this scenario.

Interoperability is defined in ISO/IEC 17788 as the "ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged." That is not the correct answer because they are planning on how to get out.

Portability is defined in ISO/IEC 17788 as the "ability to easily transfer data from one system to another without being required to re-enter the data." This is not the correct answer because they are planning on how to get out of the cloud.

Availability is defined in ISO/IEC 17788 as the "property of being accessible and usable upon demand by an authorized entity."

62.

Which of the following terms is the MOST specific when talking about a self-learning system for data classification?

Machine learning

Artificial intelligence

Data science

Blockchain

Correct answer: Machine learning

Machine learning (ML) is one part of artificial intelligence (AI). Both of these fall under the general field of data science.

Blockchain is an unrelated technology.

63.

Which of the following is at risk of being compromised when quantum computing technology matures?

RSA

Python

OWASP

The GNU Compiler Collection

Correct answer: Quantum computing

Quantum computing is capable of solving problems that traditional computers are incapable of solving. When quantum computing becomes widely accessible to the general public, it will almost certainly be via the cloud due to the substantial processing resources necessary to do quantum calculations. Once the technology matures, quantum computers could crack modern cryptographic methods.

RSA is an asymmetric cryptographic algorithm. None of the other options are types of cryptography.

Python is a programming language. OWASP is a community. The GNU Compiler Collection is a collection of free and open-source compiler software.

64.

An organization combines offerings from multiple cloud providers into a package customized to a customer's needs. Which of the following roles BEST describes this company?

Cloud Service Broker

Cloud Service Provider

Cloud Service Partner

Cloud Customer

Correct answer: Cloud Service Broker

Some of the important roles and responsibilities in cloud computing include:

- *Cloud Service Provider: The cloud service provider offers cloud services to a third party. They are responsible for operating their infrastructure and meeting service level agreements (SLAs).*
- *Cloud Customer: The cloud customer uses cloud services. They are responsible for the portion of the cloud infrastructure stack under their control.*
- *Cloud Service Partners: Cloud service partners are distinct from the cloud service provider but offer a related service. For example, a cloud service partner may offer add-on security services to secure an organization's cloud infrastructure.*
- *Cloud Service Brokers: A cloud service broker may combine services from several different cloud providers and customize them into packages that meet a customer's needs and integrate with their environment.*
- *Regulators: Regulators ensure that organizations — and their cloud infrastructures — are compliant with applicable laws and regulations. The global nature of the cloud can make regulatory and jurisdictional issues more complex.*

65.

Filippa has been assessing Hardware Security Modules (HSM) for implementation in their data center. She works for a public Cloud Service Provider (CSP), and their customers need access to such products to be able to store their cryptographic keys securely. What standard do HSMs get certified against that has four levels of certification?

Federal Information Processing Standard (FIPS) 140-3

National Institute of Standards and Technology Special Publication (NIST SP) 800-53

Payment Card Industry Data Security Standards (PCE DSS)

International Standards Organization/ International Electrotechnical Committee (ISO/IEC) 27001

Correct answer: Federal Information Processing Standard (FIPS) 140-3

The Federal Information Processing Standard (FIPS) 140-3 and the older FIPS 140-2 version are standards established by the National Institute of Standards and Technology (NIST) in the United States. It defines the security requirements for cryptographic modules used in various information systems, including computers, servers, and telecommunications equipment.

The primary goal of FIPS 140-3 is to ensure the security and integrity of sensitive information by specifying the criteria that cryptographic modules must meet. These modules encompass both hardware and software components involved in encryption, decryption, key management, and other cryptographic operations. There are four (1-4) certification levels.

NIST SP 800-53 is a publication by the National Institute of Standards and Technology (NIST) in the United States. It provides a comprehensive set of security controls and guidelines for federal information systems and organizations.

Payment Card Industry Data Security Standards (PCE DSS) is a set of security standards developed by the Payment Card Industry Security Standards Council (PCI SSC) to ensure the secure handling and protection of credit card data. PCI DSS applies to any organization that processes, stores, or transmits cardholder data. This includes merchants, service providers, financial institutions, and any entity involved in the payment card ecosystem. Compliance with PCI DSS is mandatory for these organizations to ensure the security of cardholder data and prevent unauthorized access or fraud.

ISO/IEC 27001 is an international standard for Information Security Management Systems (ISMS). It provides a systematic and comprehensive approach to managing and protecting sensitive information within an organization.

66.

Which of the following enables a cloud provider to offer services on a pay-by-usage basis?

Metered Service

On-Demand Self-Service

Multitenancy

Resource Pooling

Correct answer: Metered Service

The six common characteristics of cloud computing include:

- *Broad Network Access: Cloud services are widely available over the network, whether using web browsers, secure shell (SSH), or other protocols.*
- *On-Demand Self-Service: Cloud customers can redesign their cloud infrastructure at need, leasing additional storage or processing power or specialized components and gaining access to them on-demand.*
- *Resource Pooling: Cloud customers lease resources from a shared pool maintained by the cloud provider at need. This enables the cloud provider to take advantage of economies of scale by spreading infrastructure costs over multiple cloud customers.*
- *Rapid Elasticity and Scalability: Cloud customers can expand or contract their cloud footprint at need, much faster than would be possible if they were using physical infrastructure.*
- *Measured or Metered Service: Cloud providers measure their customers' usage of the cloud and bill them for the resources that they use.*
- *Multitenancy: Public cloud environments are multitenant, meaning that multiple different cloud customers share the same underlying infrastructure.*

67.

The term IaC relates to which of the following?

DevSecOps

ML/AI

Blockchain

Confidential Computing

Correct answer: DevSecOps

Cloud computing is closely related to many emerging technologies. Some examples include:

- *Machine Learning and Artificial Intelligence (ML/AI): Machine learning is a subset of AI and includes algorithms that are designed to learn from data and build models to identify trends, perform classifications, and other tasks. Cloud computing is linked to the rise of ML/AI because it provides the computing power needed to train the models used by ML/AI and operate these technologies at scale.*
- *Blockchain: Blockchain technology creates an immutable digital ledger in a decentralized fashion. It is used to support cryptocurrencies, track ownership of assets, and implement various other functions without relying on a centralized authority or single point of failure. Cloud computing is related to blockchain because many of the nodes used to maintain and operate blockchain networks run on cloud computing platforms.*
- *Confidential Computing: While data is commonly encrypted at rest and in transit, it is often decrypted while in use, which creates security concerns. Confidential computing involves the use of trusted execution environments (TEEs) that protect and isolate sensitive data from potential threats while in use.*
- *DevSecOps: DevSecOps is the practice of building security into automated DevOps workflows. DevSecOps can be used to secure cloud-hosted applications. Also, infrastructure as code (IaC) involves automating the configuration of cloud-based systems and servers to reduce errors and improve scalability.*

68.

Software applications such as email and customer relationship management (CRM) that are provided as a cloud service typically use which category of cloud computing as their service model?

SaaS

PaaS

IaaS

DBaaS

Correct answer: Software as a Service (SaaS)

Software as a Service (SaaS) is a type of cloud service in which the cloud provider maintains and manages everything on the back end (including the infrastructure, platform, and server OS), and the cloud customer can simply access the software without needing to do any maintenance on it. Applications like email, calendar, and CRM where end users only need access to application-level functionality typically use a SaaS model.

PaaS allows the customer to have access to a server-based or server-less environment to load their software.

IaaS allows the customer to bring all the operating systems, including routers, switches, servers, firewalls, intrusion detection systems, and so on. This allows a customer to build a virtual data center without having to worry about buying and maintaining the physical equipment.

DBaaS allows the customer to have a database without having to maintain the hardware or even the operating system that is the database.

69.

The terms "protection profile" and "evaluation assurance level (EAL)" are associated with which of the following?

Common Criteria

FIPS 140-2

FedRAMP

CSA STAR

Correct answer: Common Criteria

Cloud providers' systems may be subject to certification against standards that address a specific component, such as a cryptographic module. Examples of these system/subsystem product certifications include:

- *Common Criteria: Common Criteria (CC) are guidelines for comparing various security systems. A protection profile describes the security requirements of systems being compared, and the evaluation assurance level (EAL) describes the level of testing performed on the system, ranging from 1 (lowest) to 7 (highest).*
- *FIPS 140-2: Federal Information Processing Standard (FIPS) 140-2 is a US government standard for cryptographic modules. FIPS compliance is necessary for organizations that want to work with the US government and mandates the use of secure cryptographic algorithms like AES.*

FedRAMP and G-Cloud are standards used by the US and UK governments.

The Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) registry allows cloud service providers to register security and privacy controls. The registry provides potential customers with a way to identify cloud providers that can meet specific security requirements.

70.

Tatum has been working with a cloud data architect and cloud architect to plan the access control model. They want an implementation that will allow them to grant access based on characteristics such as job titles, department, and location.

What should they use?

ABAC

RBAC

ACL

CDAC

Correct answer: Attribute-Based Access Control (ABAC)

Attribute-Based Access Control (ABAC) grants or denies access to resources based on various attributes associated with the subjects, objects, and environmental conditions. It offers a flexible and dynamic approach to access control, allowing access decisions to be made based on a wide range of attributes rather than relying solely on user roles or permissions. Attributes can include job titles, departments, locations, data times, and more.

Role-Based Access Control (RBAC) is an access control model widely used in cloud computing environments to manage and enforce access permissions based on user roles. RBAC assigns roles to users or entities and associates permissions with those roles, allowing for simplified and efficient access management.

Access Control Lists (ACLs) are a mechanism used in computer systems and networks to define and enforce permissions or access rights for users or entities to access resources or perform specific actions. ACLs are typically associated with files, directories, network devices, or other system resources.

Content Dependent Access Control (CDAC), also known as Context-Based Access Control, is an access control mechanism that grants or denies access to resources based on the content or context of the information being accessed. Unlike traditional access control models that primarily rely on user identity or resource attributes, CDAC takes into account the actual content of the information to make access decisions.

71.

Acme DB Corp is a cloud service provider (CSP) that operates a platform as a service (PaaS) offering. The Acme DB Corp PaaS offering provides hosted PostgreSQL database access to customers. Acme DB Corp. uses type 1 hypervisors to run the virtual machines (VMs) required for the PaaS offering.

Which of the following is Acme DB Corp's responsibility in this scenario?

Secure configuration of the VMs

Secure configuration of the databases

Efficiency of SQL queries

Database schema changes

Correct answer: Secure configuration of the VMs

In this PaaS model, the customer is responsible for securely configuring databases, writing efficient SQL queries, and modifying database schemas.

The cloud service provider, Acme DB Corp, is responsible for the underlying infrastructure, including VM updates and configuration.

72.

Your organization currently hosts its cloud environment in the organization's data center. The organization utilizes a provider for their backup solution in accordance with their business continuity plan. Which configuration BEST describes their deployment?

Private cloud, cloud service backup

Private cloud, private backup

Cloud service backup, private backup

Cloud service backup, third-party backup

Correct answer: Private cloud, cloud service backup

The organization is using their own private data center for their cloud, which is a private cloud. It is not necessary to have the private cloud within their own data center, but that is what's mentioned in the question.

They are then backing up their cloud using a public provider, which is the cloud service backup answer option. Therefore, answers that have private backup are not correct.

The answers that have cloud service backup and/or third-party backup are not correct because there is only the cloud service backup in the question.

73.

In which of the following cloud service models does the cloud provider offer an environment where the customer can build and deploy applications and the provider manages compute, data storage, and other dependencies?

PaaS

SaaS

IaaS

FaaS

Correct answer: PaaS

Cloud services are typically provided under three main service models:

- *Software as a Service (SaaS): Under the SaaS model, the cloud provider offers the customer access to a complete application developed by the cloud provider. Webmail services like Google Workspace and Microsoft 365 are examples of SaaS offerings.*
- *Platform as a Service (PaaS): In a PaaS model, the cloud provider offers the customer a managed environment where they can build and deploy applications. The cloud provider manages compute, data storage, and other services for the application.*
- *Infrastructure as a Service (IaaS): In IaaS, the cloud provider offers an environment where the customer has access to various infrastructure building blocks. AWS, which allows customers to deploy virtual machines (VMs) or use block data storage in the cloud, is an example of an IaaS platform.*

Function as a Service (FaaS) is a form of PaaS in which the customer creates individual functions that can run in the cloud. Examples include AWS Lambda, Microsoft Azure Functions, and Google Cloud Functions.

74.

A cloud administrator needs to rapidly deploy an application package throughout a large cloud environment. Which of the following could this engineer use to accomplish this easily?

Containers

Key management

Mobile Device Management (MDM)

Hypervisor

Correct answer: Containers

A wrapper that contains all the configuration, code, and libraries needed for an application, which can be rapidly deployed across a cloud environment, is known as a container.

Virtual Machines (VMs) can be built on a hypervisor. On the virtual machine, the software can be loaded. This is not the best answer because of the word rapidly in the question. VMs are not as fast and easy to manage as containers.

Key management is for storing and protecting cryptographic keys. They are likely used somewhere in the application, but that is not the focus of the question. Deployment is the question.

MDM software is used to manage mobile devices. It gives the administrators the ability to contain corporate data on a personal phone. Data can be deleted and the phone can be wiped when needed, among other features.

75.

Which of the following statements about type 1 hypervisors is TRUE?

Because they run directly on a physical server, type 1 hypervisors have a smaller attack surface than type 2 hypervisors

Because they run directly on a host operating system, type 1 hypervisors have a larger attack surface than type 2 hypervisors

Because they run directly on a physical server, type 1 hypervisors have a larger attack surface than type 2 hypervisors

Because they run directly on a host operating system, type 1 hypervisors are not susceptible to VM escape attacks

---

Correct answer: Because they run directly on a physical server, type 1 hypervisors have a smaller attack surface than type 2 hypervisors

Type 1 hypervisors are known as bare-metal hypervisors because they run directly on the physical hardware of the machine, and they are not software-based like type 2 hypervisors. Because they are tied to the hardware, they are considered the operating system of the server and should be designed as thinly as possible. That means they have a smaller attack surface than type 2 hypervisors, which run on a host operating system and therefore have a larger attack surface, more complexity, and more opportunities to inject malicious code.

Both types of hypervisors can be susceptible to VM escape attacks.

76.

Which of the following network security controls might require access to mirroring services provided by the cloud provider?

Traffic Inspection

Network Security Groups

Geofencing

Zero Trust Network

Correct answer: Traffic Inspection

Network security controls that are common in cloud environments include:

- *Network Security Groups: Network security groups (NSGs) limit access to certain resources, such as firewalls or sensitive VMs or databases. This makes it more difficult for an attacker to access these resources during their attacks.*
- *Traffic Inspection: In the cloud, traffic monitoring can be complex since traffic is often sent directly to virtual interfaces. Many cloud environments have traffic mirroring solutions that allow an organization to see and analyze all traffic to its cloud-based resources.*
- *Geofencing: Geofencing limits the locations from which a resource can be accessed. This is a helpful security control in the cloud, which is accessible from anywhere.*
- *Zero Trust Network: Zero trust networks apply the principle of least privilege, where users, applications, systems, etc., are only granted the access and permissions that they need for their jobs. All requests for access to resources are individually evaluated, so an entity can only access those resources for which they have the proper permissions.*

77.

A cloud customer who has been using a Hardware Security Module (HSM) is migrating to a newer model. They want to ensure that their keys will never be recovered by anyone, so they are taking actions to ensure that. One of the steps that they are taking is to overwrite the erased data with arbitrary data and zero values.

What are they doing?

Zeroization

Cryptographic erasure

Degaussing

Data hijacking

Correct answer: Zeroization

Zeroization is another term for overwriting. In this process, erased data is overwritten with arbitrary data and zero values as a means of data sanitation.

Cryptographic erasure is when data is encrypted, and then the key that was used is destroyed. This is a possible option for customers when they do not have access to the drives themselves that their data resides on, which would be true for PaaS, SaaS, and possibly IaaS in public clouds.

Degaussing is a process of disrupting the magnetic state on magnetic drives—Hard Disk Drives (HDD). It does render a drive unusable. It would be possible for the cloud provider to perform this sanitization or possibly in a private cloud.

Data hijacking is an odd term, but it means that the bad actors of the world are taking control of someone's data. Something like ransomware would be like this.

78.

The ability to deploy VMs and use block data storage in the cloud is a feature of which cloud service model?

IaaS

PaaS

SaaS

FaaS

Correct answer: IaaS

Cloud services are typically provided under three main service models:

- *Software as a Service (SaaS): Under the SaaS model, the cloud provider offers the customer access to a complete application developed by the cloud provider. Webmail services like Google Workspace and Microsoft 365 are examples of SaaS offerings.*
- *Platform as a Service (PaaS): In a PaaS model, the cloud provider offers the customer a managed environment where they can build and deploy applications. The cloud provider manages compute, data storage, and other services for the application.*
- *Infrastructure as a Service (IaaS): In IaaS, the cloud provider offers an environment where the customer has access to various infrastructure building blocks. AWS, which allows customers to deploy virtual machines (VMs) or use block data storage in the cloud, is an example of an IaaS platform.*

Function as a Service (FaaS) is a form of PaaS in which the customer creates individual functions that can run in the cloud. Examples include AWS Lambda, Microsoft Azure Functions, and Google Cloud Functions.

79.

A cloud architect wants to move all their organization's physical hardware to the cloud. This includes routers, switches, firewalls, and servers. They are looking for a service that will allow them to manage the operating systems of the servers and all the applications that will be installed on the servers. However, they no longer want to have to manage any physical hardware.

Which type of cloud provider would BEST suit this cloud architect's needs?

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Database as a Service (DBaaS)

Software as a Service (SaaS)

Correct answer: Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) providers will provide cloud customers with everything they need from a hardware standpoint, including routers, switches, firewalls, and servers. The customer will still be responsible for managing all the software and operating systems but will not need to manage any hardware. IaaS allows a customer to effectively build a virtual data center in the cloud. The actual hardware equipment purchase and maintenance is removed from the customer's point of view, but the customer can bring the Operating Systems (OS), which are routers, switches, firewalls, etc.

PaaS is an OS or platform at a time if it is server-based. This would not include routers and switches though. There is also server-less, in which case the customer does not even need to worry about the OS at all.

DBaaS is just a database, as the name implies. There is no configuration of the routers or switches. This would be considered PaaS.

SaaS is the furthest removed from the question. The network equipment, routers, switches, and so on as well as the OS for the servers and the administration of the software itself is all under the cloud provider's control. It does not allow the customer to do anything other than use the software.

80.

Which of these cloud-related factors is MOST related to an organization's ability to implement an integrated multi-cloud architecture?

Interoperability

Portability

Reversibility

Resiliency

Correct answer: Interoperability

Interoperability is defined, in ISO/IEC 17788, as “the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged." If a specific cloud provider has some specific format that the virtual machine image (for Infrastructure as a Service [IaaS]) or how the data is stored in Platform and Software as a Service (PaaS and SaaS), then it may be difficult to connect or move apps across multi-cloud environments.

Portability is the ability to transfer data from one system to another without having to re-enter the data. While this might be related to multi-cloud infrastructure, it is less so than interoperability.

Reversibility is defined in ISO/IEC 17788 as the "process for cloud service customers to retrieve their cloud service customer data and application artifacts and for the cloud service provider to delete all cloud service customer data as well as contractually specified cloud service derived data after an agreed period."

Resiliency is about maintaining a specific level of service.

81.

Cloud service providers will have clear requirements for items such as uptime, customer service response time, and availability. Where would these requirements MOST LIKELY be outlined for the client?

SLA

PLA

SOW

MSA

Correct answer: SLA

Requirements such as uptime, customer service response time, and availability should be outlined in a service level agreement (SLA). When a provider doesn't meet their SLA requirements, it could lead to termination of the contract or financial benefits to the cloud customer.

Privacy level agreements (PLAs), business associate agreements (BAAs), and data processing agreements (DPAs) are all fundamentally the same. They are all agreements like an SLA but about the privacy requirements to protect the personal data or Personally Identifiable Information (PII) that will be stored and processed on the cloud provider's equipment. DPA is the term used in the European Union under the General Data Protection Regulation (GDPR). HIPAA in the USA requires a BAA. PLA is a generic term for anywhere else.

A statement of work (SOW) defines details for a specific project. SOWs typically reference a master service agreement (MSA) between the client and vendor.

82.

Which of the following is TRUE in terms of maintenance and versioning in the cloud?

The Cloud Service Customer (CSC) is responsible for the maintenance and versioning of the apps they acquire and develop in a Platform as a Service (PaaS) solution. The Cloud Service Provider (CSP) is responsible for the platform, tools, and underlying infrastructure.

The Cloud Service Customer (CSC) is responsible for the maintenance and versioning of all components in a Software as a Service (SaaS) product. The Cloud Service Provider (CSP) is responsible for the Virtual Machines (VM) and their patches.

The Cloud Service Customer (CSC) is responsible for the maintenance and versioning of the network and storage as well as the virtualization software in an Infrastructure as a Service (IaaS) solution. The Cloud Service Provider (CSP) is responsible for the physical security of the Data Center (DC).

Updates and patches are scheduled with the customer in the Software as a Service (SaaS) and Platform as a Service (PaaS) model. The Cloud Service Provider (CSP) is responsible for the virtualization software and the underlying infrastructure.

Correct answer: The Cloud Service Customer (CSC) is responsible for the maintenance and versioning of the apps they acquire and develop in a Platform as a Service (PaaS) solution. The Cloud Service Provider (CSP) is responsible for the platform, tools, and underlying infrastructure.

In IaaS, the cloud provider is responsible for the security of the DC, the underlying infrastructure of routers, switches, and servers. The CSC is responsible for the Operating Systems (OS) that make up the virtual infrastructure, the middleware, software, and data.

In PaaS, the cloud provider is still responsible for the above mentioned and the platform and tools. The CSC is responsible for all the middleware and software they add to the platform (if server-based PaaS) and their data.

In SaaS, the cloud provider is also responsible for what was mentioned two paragraphs above plus the software that the customer uses. The CSC is responsible for their data.

The answer "The Cloud Service Customer (CSC) is responsible for the maintenance and versioning of all components in a Software as a Service (SaaS) product. The Cloud Service Provider (CSP) is responsible for the Virtual Machines (VM) and their patches" is wrong because the CSC is not responsible for the software.

The answer "The Cloud Service Customer (CSC) is responsible for the maintenance and versioning of the network and storage as well as the virtualization software in an Infrastructure as a Service (IaaS) solution. The Cloud Service Provider (CSP) is responsible for the physical security of the Data Center (DC)" is wrong because the CSC is not responsible for the virtualization software. If the network and storage here are physical, they are not responsible. If they are virtual, the CSC is responsible.

The answer "Updates and patches are scheduled with the customer in the Software as a Service (SaaS) and Platform as a Service (PaaS) model. The Cloud Service Provider (CSP) is responsible for the virtualization software and the underlying infrastructure" is wrong because the provider does not schedule software updates with the CSC in a SaaS. In PaaS, the CSC is responsible for the software updates, and the provider may or may not be responsible for the OS updates.

83.

Cloud environments offered by a cloud services provider that are compliant with Federal Risk and Authorization Management Program (FedRAMP) are MOST likely to be an example of which of the following?

Community cloud

Hybrid cloud

Public cloud

Multi-cloud

Correct answer: Community Cloud

Cloud services are available under a few different deployment models, including:

- *Private cloud: In private clouds, the cloud customer builds their own cloud in-house or has a provider do so for them. Private clouds have dedicated servers, making them more secure but also more expensive.*
- *Public cloud: Public clouds are multi-tenant environments where multiple cloud customers share the same infrastructure managed by a third-party provider.*
- *Hybrid cloud: Hybrid cloud deployments mix both public and private cloud infrastructure. This allows data and applications to be hosted on the cloud that makes the most sense for them.*
- *Multi-cloud: Multi-cloud environments use cloud services from multiple different cloud providers. This enables customers to take advantage of price differences or optimizations offered by different providers.*
- *Community cloud: A community cloud is essentially a private cloud used by a group of related organizations rather than a single organization. It could be operated by that group or a third party, such as FedRAMP-compliant cloud environments operated by cloud service providers.*

84.

We have been working with different Artificial Intelligence (AI) methods for years. While we may not be at a true AI just yet, there have been several great advances in this technology. Which method has the software working to understand, interpret, and generate text that seems to be from a live human?

Natural Language Processing (NLP)

Deep Learning (DL)

Machine Learning (ML)

Bayesian Networks

Correct answer: Natural Language Processing (NLP)

Natural Language Processing (NLP) focuses on enabling computers to understand, interpret, and generate human language. NLP methods involve techniques such as text classification, sentiment analysis, named entity recognition, machine translation, and question-answering systems.

AI methods, such as the one above (NLP) and the three below (the other answer options) refer to the various techniques and approaches used in the field of Artificial Intelligence to solve problems, make predictions, and perform tasks that typically require human intelligence. These methods encompass a broad range of algorithms, models, and methodologies that enable machines to learn, reason, and make decisions autonomously.

Machine Learning (ML) is a subset of AI that focuses on designing algorithms and models that allow computers to learn from data without being explicitly programmed. ML methods include supervised learning, unsupervised learning, and reinforcement learning, where algorithms learn patterns and make predictions based on training examples or feedback.

Deep Learning (DL) is a subfield of ML that involves training artificial neural networks with multiple layers to recognize patterns and extract complex representations from data. DL methods, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have been particularly successful in image recognition, natural language processing, and other complex tasks.

Bayesian networks are probabilistic graphical models that represent relationships among variables using a directed acyclic graph. They apply Bayesian inference to

update beliefs and make predictions based on observed evidence and prior knowledge.

85.

What is the first stage of the cloud data lifecycle?

- **Create**
- Plan
- Generate
- Use

Correct answer: Create

The cloud data lifecycle consists of six phases. They are:

1. ***Create** - Initial data creation*
2. ***Store** - Data is saved in a system where it can be retrieved in the future*
3. ***Use** - Data is retrieved and used*
4. ***Share** - Users are granted permission to use the data*
5. ***Archive** - Data is moved to a long-term storage location*
6. ***Destroy** - Permanent deletion*

Plan and generate are distractor answers.

86.

Obert is building a private cloud for his corporation with the assistance of many different departments. As they install hypervisors and begin to provision accounts to create virtual machines for different departments, he is wondering if they would be a single tenant or a multi-tenant environment. In a private cloud environment, are there still multiple tenants?

Yes, there could be. A tenancy isolates data and virtual machines from other tenants. These can be different groups within the organization.

Yes, there could be. A tenancy isolates data and virtual machines from other tenants. These would be the different users within each department.

No, there would not be. A tenant isolates customers from each other, and there is technically only one customer involved in a private cloud.

No, there would not be. A tenant isolates data services from each other. There is only one company involved when you build a private cloud.

Correct answer: Yes, there could be. A tenancy isolates data and virtual machines from other tenants. These can be different groups within the organization.

According to ISO/IEC 17788, multi-tenancy allows virtual and physical resources to be allocated so that each tenant does not see the others' computations, virtual machines, applications, or data. In public clouds, it is normal that there are different customers of the cloud provider. However, in a private cloud, these tenants could/would represent the different groups within the organization.

ISO/IEC 17788 is a free document and a good, quick read for preparation for this test.

87.

What is an essential layer around a virtual machine, subnet, or cloud resource as part of a layered defense strategy?

Network security group

Ingress and egress monitoring

Cloud gateway

Contextual-based security

Correct answer: Network security group

A Network Security Group (NSG) protects a group of cloud resources. It provides a set of security rules or virtual firewall for those resources. This gives the customer additional control over security.

A cloud gateway adds an additional layer of security by transferring data between the customer and the CSP away from the public internet.

Contextual-based security leverages contextual information such as identification to assist in securing cloud resources.

External access attempts from the public internet can be blocked by ingress controls. Egress controls are a technique for preventing internal resources from connecting to unauthorized and potentially harmful websites.

88.

Poorly secured Internet of Things (IoT) devices often become part of what type of malicious network?

Botnet

DDoS

Honeynet

DoS

Correct answer: Botnet

The Internet of Things (IoT) refers to non-traditional computing devices (e.g., lamps, thermostats, and other home appliances) accessing the internet. Although some do consider laptops, smartphones, and computers to be part of IoT, for the exam, these items are unlikely to be considered part of the IoT. Poorly secured IoT devices are at risk of becoming part of a botnet that is used to carry out distributed denial of service (DDoS) attacks. The botnet is the malicious network of devices, while DDoS is the type of attack.

Denial of service (DoS) is a category of attacks that includes DDoS. A honeynet is a network set up to attract attackers.