

ISC2

Exam Questions CCSP

Certified Cloud Security Professional



NEW QUESTION 1

- (Exam Topic 4)

All of the following are techniques to enhance the portability of cloud data, in order to minimize the potential of vendor lock-in except:

- A. Ensure there are no physical limitations to moving
- B. Use DRM and DLP solutions widely throughout the cloud operation
- C. Ensure favorable contract terms to support portability
- D. Avoid proprietary data formats

Answer: B

Explanation:

DRM and DLP are used for increased authentication/access control and egress monitoring, respectively, and would actually decrease portability instead of enhancing it.

NEW QUESTION 2

- (Exam Topic 4)

The cloud customer will have the most control of their data and systems, and the cloud provider will have the least amount of responsibility, in which cloud computing arrangement?

- A. IaaS
- B. SaaS
- C. Community cloud
- D. PaaS

Answer: A

Explanation:

IaaS entails the cloud customer installing and maintaining the OS, programs, and data; PaaS has the customer installing programs and data; in SaaS, the customer only uploads data. In a community cloud, data and device owners are distributed.

NEW QUESTION 3

- (Exam Topic 4)

Which of the following areas of responsibility always falls completely under the purview of the cloud provider, regardless of which cloud service category is used?

- A. Infrastructure
- B. Data
- C. Physical
- D. Governance

Answer: C

Explanation:

Regardless of the cloud service category used, the physical environment is always the sole responsibility of the cloud provider. In many instances, the cloud provider will supply audit reports or some general information about their physical security practices, especially to those customers or potential customers that may have regulatory requirements, but otherwise the cloud customer will have very little insight into the physical environment. With IaaS, the infrastructure is a shared responsibility between the cloud provider and cloud customer. With all cloud service categories, the data and governance are always the sole responsibility of the cloud customer.

NEW QUESTION 4

- (Exam Topic 4)

Which cloud service category most commonly uses client-side key management systems?

- A. Software as a Service
- B. Infrastructure as a Service
- C. Platform as a Service
- D. Desktop as a Service

Answer: A

Explanation:

SaaS most commonly uses client-side key management. With this type of implementation, the software for doing key management is supplied by the cloud provider, but is hosted and run by the cloud customer. This allows for full integration with the SaaS implementation, but also provides full control to the cloud customer. Although the cloud provider may offer software for performing key management to the cloud customers, with the Infrastructure, Platform, and Desktop as a Service categories, the customers would largely be responsible for their own options and implementations and would not be bound by the offerings from the cloud provider.

NEW QUESTION 5

- (Exam Topic 4)

What is the intellectual property protection for a confidential recipe for muffins?

- A. Patent
- B. Trademark
- C. Trade secret
- D. Copyright

Answer:

C

Explanation:

Confidential recipes unique to the organization are trade secrets. The other answers listed are answers to other questions.

NEW QUESTION 6

- (Exam Topic 4)

Which of the following roles is responsible for creating cloud components and the testing and validation of services?

- A. Cloud auditor
- B. Inter-cloud provider
- C. Cloud service broker
- D. Cloud service developer

Answer: D

Explanation:

The cloud service developer is responsible for developing and creating cloud components and services, as well as for testing and validating services.

NEW QUESTION 7

- (Exam Topic 4)

Which of the following concepts is NOT one of the core components to an encryption system architecture?

- A. Software
- B. Network
- C. Keys
- D. Data

Answer: B

Explanation:

The network utilized is not one of the key components of an encryption system architecture. In fact, a network is not even required for encryption systems or the processing and protection of data. The data, software used for the encryption engine itself, and the keys used to implement the encryption are all core components of an encryption system architecture.

NEW QUESTION 8

- (Exam Topic 4)

The most pragmatic option for data disposal in the cloud is which of the following?

- A. Cryptoshredding
- B. Overwriting
- C. Cold fusion
- D. Melting

Answer: A

Explanation:

We don't have physical ownership, control, or even access to the devices holding the data, so physical destruction, including melting, is not an option. Overwriting is a possibility, but it is complicated by the difficulty of locating all the sectors and storage areas that might have contained our data, and by the likelihood that constant backups in the cloud increase the chance we'll miss something as it's being overwritten. Cryptoshredding is the only reasonable alternative. Cold fusion is a red herring.

NEW QUESTION 9

- (Exam Topic 4)

Which of the following provides assurance, to a predetermined acceptable level of certainty, that an entity is indeed who they claim to be?

- A. Authentication
- B. Identification
- C. Proofing
- D. Authorization

Answer: A

Explanation:

Authentication goes a step further than identification by providing a means for proving an entity's identification. Authentication is most commonly done through mechanisms such as passwords. Identification involves ascertaining who the entity is, but without a means of proving it, such as a name or user ID. Authorization occurs after authentication and sets access permissions and other privileges within a system or application for the user. Proofing is not a term that is relevant to the question.

NEW QUESTION 10

- (Exam Topic 4)

Tokenization requires two distinct _____.

- A. Personnel
- B. Authentication factors
- C. Encryption keys
- D. Databases

Answer: D

Explanation:

In order to implement tokenization, there will need to be two databases: the database containing the raw, original data, and the token database containing tokens that map to original data. Having two-factor authentication is nice, but certainly not required. Encryption keys are not necessary for tokenization. Two-person integrity does not have anything to do with tokenization.

NEW QUESTION 10

- (Exam Topic 4)

Cryptographic keys for encrypted data stored in the cloud should be _____.

- A. Not stored with the cloud provider.
- B. Generated with redundancy
- C. At least 128 bits long
- D. Split into groups

Answer: A

Explanation:

Cryptographic keys should not be stored along with the data they secure, regardless of key length. We don't split crypto keys or generate redundant keys (doing so would violate the principle of secrecy necessary for keys to serve their purpose).

NEW QUESTION 11

- (Exam Topic 4)

DLP solutions can aid in deterring loss due to which of the following?

- A. Inadvertent disclosure
- B. Natural disaster
- C. Randomization
- D. Device failure

Answer: A

Explanation:

DLP solutions may protect against inadvertent disclosure. Randomization is a technique for obscuring data, not a risk to data. DLP tools will not protect against risks from natural disasters, or against impacts due to device failure.

NEW QUESTION 16

- (Exam Topic 4)

Which of the following best describes SAML?

- A. A standard used for directory synchronization
- B. A standard for developing secure application management logistics
- C. A standard for exchanging usernames and passwords across devices.
- D. A standards for exchanging authentication and authorization data between security domains.

Answer: D

NEW QUESTION 20

- (Exam Topic 4)

Which component of ITIL involves handling anything that can impact services for either internal or public users?

- A. Incident management
- B. Deployment management
- C. Problem management
- D. Change management

Answer: A

Explanation:

Incident management is focused on limiting the impact of disruptions to an organization's services or operations, as well as returning their state to full operational status as soon as possible. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur. Deployment management is a subcomponent of change management and is where the actual code or configuration change is put into place. Change management involves the processes and procedures that allow an organization to make changes to its IT systems and services in a controlled manner.

NEW QUESTION 21

- (Exam Topic 4)

Which of the following best describes data masking?

- A. A method for creating similar but inauthentic datasets used for software testing and user training.
- B. A method used to protect prying eyes from data such as social security numbers and credit card data.
- C. A method where the last few numbers in a dataset are not obscure
- D. These are often used for authentication.
- E. Data masking involves stripping out all digits in a string of numbers so as to obscure the original number.

Answer: A

Explanation:

All of these answers are actually correct, but A is the best answer, because it is the most general, includes the others, and is therefore the optimum choice. This is a good example of the type of question that can appear on the actual exam.

NEW QUESTION 23

- (Exam Topic 4)

Which of the following technologies is NOT commonly used for accessing systems and services in a cloud environment in a secure manner?

- A. KVM
- B. HTTPS
- C. VPN
- D. TLS

Answer: A

Explanation:

A keyboard-video-mouse (KVM) system is commonly used for directly accessing server terminals in a data center. It is not a method that would be possible within a cloud environment, primarily due to the use of virtualized systems, but also because only the cloud provider's staff would be allowed the physical access to hardware systems that's provided by a KVM. Hypertext Transfer Protocol Secure (HTTPS), virtual private network (VPN), and Transport Layer Security (TLS) are all technologies and protocols that are widely used with cloud implementations for secure access to systems and services.

NEW QUESTION 25

- (Exam Topic 4)

What is the intellectual property protection for a useful manufacturing innovation?

- A. Trademark
- B. Copyright
- C. patent
- D. Trade secret

Answer: C

Explanation:

Patents protect processes (as well as inventions, new plantlife, and decorative patterns). The other answers listed are answers to other questions.

NEW QUESTION 27

- (Exam Topic 4)

The different cloud service models have varying levels of responsibilities for functions and operations depending with the model's level of service. In which of the following models would the responsibility for patching lie predominantly with the cloud customer?

- A. DaaS
- B. SaaS
- C. PaaS
- D. IaaS

Answer: D

Explanation:

With Infrastructure as a Service (IaaS), the cloud customer is responsible for deploying and maintaining its own systems and virtual machines. Therefore, the customer is solely responsible for patching and any other security updates it finds necessary. With Software as a Service (SaaS), Platform as a Service (PaaS), and Desktop as a Service (DaaS), the cloud provider maintains the infrastructure components and is responsible for maintaining and patching them.

NEW QUESTION 30

- (Exam Topic 4)

All of the following are terms used to describe the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:

- A. Tokenization
- B. Masking
- C. Data discovery
- D. Obfuscation

Answer: C

Explanation:

Data discovery is a term used to describe the process of identifying information according to specific traits or categories. The rest are all methods for obscuring data.

NEW QUESTION 35

- (Exam Topic 4)

What's a potential problem when object storage versus volume storage is used within IaaS for application use and dependency?

- A. Object storage is only optimized for small files.
- B. Object storage is its own system, and data consistency depends on replication.
- C. Object storage may have availability issues.
- D. Object storage is dependent on access control from the host server.

Answer: B

Explanation:

Object storage runs on its own independent systems, which have their own redundancy and distribution. To ensure data consistency, sufficient time is needed for objects to fully replicate to all potential locations before being accessed. Object storage is optimized for high availability and will not be any less reliable than any other virtual machine within a cloud environment. It is hosted on a separate system that does not have dependencies in local host servers for access control, and it is optimized for files of all different sizes and uses.

NEW QUESTION 39

- (Exam Topic 4)

All policies within the organization should include a section that includes all of the following, except:

- A. Policy adjudication
- B. Policy maintenance
- C. Policy review
- D. Policy enforcement

Answer: A

Explanation:

All the elements except adjudication need to be addressed in each policy. Adjudication is not an element of policy.

NEW QUESTION 41

- (Exam Topic 4)

Because of multitenancy, specific risks in the public cloud that don't exist in the other cloud service models include all the following except:

- A. DoS/DDoS
- B. Information bleed
- C. Risk of loss/disclosure due to legal seizures
- D. Escalation of privilege

Answer: A

Explanation:

DoS/DDoS threats and risks are not unique to the public cloud model.

NEW QUESTION 44

- (Exam Topic 4)

What masking strategy involves the replacing of sensitive data at the time it is accessed and used as it flows between the data and application layers of a service?

- A. Active
- B. Static
- C. Dynamic
- D. Transactional

Answer: C

Explanation:

Dynamic masking involves the live replacing of sensitive data fields during transactional use between the data and application layers of a service. Static masking involves creating a full data set with the sensitive data fields masked, but is not done during live transactions like dynamic masking. Active and transactional are offered as similar types of answers but are not types of masking.

NEW QUESTION 49

- (Exam Topic 4)

With an application hosted in a cloud environment, who could be the recipient of an eDiscovery order?

- A. Users
- B. Both the cloud provider and cloud customer
- C. The cloud customer
- D. The cloud provider

Answer: B

Explanation:

Either the cloud customer or the cloud provider could receive an eDiscovery order, and in almost all circumstances they would need to work together to ensure compliance.

NEW QUESTION 50

- (Exam Topic 4)

You need to gain approval to begin moving your company's data and systems into a cloud environment. However, your CEO has mandated the ability to easily remove your IT assets from the cloud provider as a precondition.

Which of the following cloud concepts would this pertain to?

- A. Removability
- B. Extraction
- C. Portability
- D. Reversibility

Answer: D

Explanation:

Reversibility is the cloud concept involving the ability for a cloud customer to remove all of its data and IT assets from a cloud provider. Also, processes and agreements would be in place with the cloud provider that ensure all removals have been completed fully within the agreed upon timeframe. Portability refers to the ability to easily move between different cloud providers and not be locked into a specific one. Removability and extraction are both provided as terms similar to reversibility, but neither is the official term or concept.

NEW QUESTION 51

- (Exam Topic 4)

Which format is the most commonly used standard for exchanging information within a federated identity system?

- A. XML
- B. HTML
- C. SAML
- D. JSON

Answer: C

Explanation:

Security Assertion Markup Language (SAML) is the most common data format for information exchange within a federated identity system. It is used to transmit and exchange authentication and authorization data. XML is similar to SAML, but it's used for general-purpose data encoding and labeling and is not used for the exchange of authentication and authorization data in the way that SAML is for federated systems. JSON is used similarly to XML, as a text-based data exchange format that typically uses attribute-value pairings, but it's not used for authentication and authorization exchange. HTML is used only for encoding web pages for web browsers and is not used for data exchange--and certainly not in a federated system.

NEW QUESTION 52

- (Exam Topic 4)

The baseline should cover which of the following?

- A. Data breach alerting and reporting
- B. All regulatory compliance requirements
- C. As many systems throughout the organization as possible
- D. A process for version control

Answer: C

Explanation:

The more systems that be included in the baseline, the more cost-effective and scalable the baseline is. The baseline does not deal with breaches or version control; those are the provinces of the security office and CMB, respectively. Regulatory compliance might (and usually will) go beyond the baseline and involve systems, processes, and personnel that are not subject to the baseline.

NEW QUESTION 57

- (Exam Topic 4)

Which of the following could be used as a second component of multifactor authentication if a user has an RSA token?

- A. Access card
- B. USB thumb drive
- C. Retina scan
- D. RFID

Answer: C

Explanation:

A retina scan could be used in conjunction with an RSA token because it is a biometric factor, and thus a different type of factor. An access card, RFID, and USB thumb drive are all items in possession of a user, the same as an RSA token, and as such would not be appropriate.

NEW QUESTION 62

- (Exam Topic 4)

The application normative framework is best described as which of the following?

- A. A superset of the ONF
- B. A stand-alone framework for storing security practices for the ONF
- C. The complete ONF
- D. A subnet of the ONF

Answer: D

Explanation:

Remember, there is a one-to-many ratio of ONF to ANF; each organization has one ONF and many ANFs (one for each application in the organization). Therefore, the ANF is a subset of the ONF.

NEW QUESTION 64

- (Exam Topic 4)

Key maintenance and security are paramount within a cloud environment due to the widespread use of encryption for both data and transmissions.

Which of the following key-management systems would provide the most robust control over and ownership of the key-management processes for the cloud customer?

- A. Remote key management service

- B. Local key management service
- C. Client key management service
- D. Internal key management service

Answer: A

Explanation:

A remote key management system resides away from the cloud environment and is owned and controlled by the cloud customer. With the use of a remote service, the cloud customer can avoid being locked into a proprietary system from the cloud provider, but also must ensure that service is compatible with the services offered by the cloud provider. A local key management system resides on the actual servers using the keys, which does not provide optimal security or control over them. Both the terms internal key management service and client key management service are provided as distractors.

NEW QUESTION 66

- (Exam Topic 4)

What are SOC 1/SOC 2/SOC 3?

- A. Audit reports
- B. Risk management frameworks
- C. Access controls
- D. Software developments

Answer: A

Explanation:

An SOC 1 is a report on controls at a service organization that may be relevant to a user entity's internal control over financial reporting. An SOC 2 report is based on the existing SysTrust and WebTrust principles. The purpose of an SOC 2 report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, or privacy. An SOC 3 report is also based on the existing SysTrust and WebTrust principles, like a SOC 2 report. The difference is that the SOC 3 report does not detail the testing performed.

NEW QUESTION 69

- (Exam Topic 4)

Which of the following is NOT one of the components of multifactor authentication?

- A. Something the user knows
- B. Something the user has
- C. Something the user sends
- D. Something the user is

Answer: C

Explanation:

Multifactor authentication systems are composed of something the user knows, has, and/or is, not something the user sends. Multifactor authentication commonly uses something that a user knows, has, and/or is (such as biometrics or features).

NEW QUESTION 71

- (Exam Topic 4)

Which of the following are considered to be the building blocks of cloud computing?

- A. CPU, RAM, storage, and networking
- B. Data, CPU, RAM, and access control
- C. Data, access control, virtualization, and services
- D. Storage, networking, printing, and virtualization

Answer: A

NEW QUESTION 74

- (Exam Topic 4)

Data masking can be used to provide all of the following functionality, except:

- A. Secure remote access
- B. test data in sandboxed environments
- C. Authentication of privileged users
- D. Enforcing least privilege

Answer: C

Explanation:

Data masking does not support authentication in any way. All the others are excellent use cases for data masking.

NEW QUESTION 75

- (Exam Topic 4)

When reviewing the BIA after a cloud migration, the organization should take into account new factors related to data breach impacts. One of these new factors is:

- A. Many states have data breach notification laws.
- B. Breaches can cause the loss of proprietary data.
- C. Breaches can cause the loss of intellectual property.
- D. Legal liability can't be transferred to the cloud provider.

Answer: D

Explanation:

State notification laws and the loss of proprietary data/intellectual property pre-existed the cloud; only the lack of ability to transfer liability is new.

NEW QUESTION 80

- (Exam Topic 4)

In a cloud environment, encryption should be used for all the following, except:

- A. Secure sessions/VPN
- B. Long-term storage of data
- C. Near-term storage of virtualized images
- D. Profile formatting

Answer: D

Explanation:

All of these activities should incorporate encryption, except for profile formatting, which is a made-up term.

NEW QUESTION 81

- (Exam Topic 4)

All of these are methods of data discovery, except:

- A. Label-based
- B. User-based
- C. Content-based
- D. Metadata-based

Answer: B

Explanation:

All the others are valid methods of data discovery; user-based is a red herring with no meaning.

NEW QUESTION 83

- (Exam Topic 4)

Which of the following would be considered an example of insufficient due diligence leading to security or operational problems when moving to a cloud?

- A. Monitoring
- B. Use of a remote key management system
- C. Programming languages used
- D. Reliance on physical network controls

Answer: D

Explanation:

Many organizations in a traditional data center make heavy use of physical network controls for security. Although this is a perfectly acceptable best practice in a traditional data center, this reliance is not something that will port to a cloud environment. The failure of an organization to properly understand and adapt to the difference in network controls when moving to a cloud will likely leave an application with security holes and vulnerabilities. The use of a remote key management system, monitoring, or certain programming languages would not constitute insufficient due diligence by itself.

NEW QUESTION 86

- (Exam Topic 4)

A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence. Which core concept of cloud computing is most related to vendor lock-in?

- A. Scalability
- B. Interoperability
- C. Portability
- D. Reversibility

Answer: C

Explanation:

Portability is the ability for a cloud customer to easily move their systems, services, and applications among different cloud providers. By avoiding reliance on proprietary APIs and other vendor-specific cloud features, an organization can maintain flexibility to move among the various cloud providers with greater ease. Reversibility refers to the ability for a cloud customer to quickly and easily remove all their services and data from a cloud provider. Interoperability is the ability to reuse services and components for other applications and uses. Scalability refers to the ability of a cloud environment to add or remove resources to meet current demands.

NEW QUESTION 89

- (Exam Topic 4)

In a federated identity arrangement using a trusted third-party model, who is the identity provider and who is the relying party?

- A. The users of the various organizations within the federations within the federation/a CASB
- B. Each member organization/a trusted third party
- C. Each member organization/each member organization
- D. A contracted third party/the various member organizations of the federation

Answer: D

Explanation:

In a trusted third-party model of federation, each member organization outsources the review and approval task to a third party they all trust. This makes the third party the identifier (it issues and manages identities for all users in all organizations in the federation), and the various member organizations are the relying parties (the resource providers that share resources based on approval from the third party).

NEW QUESTION 94

- (Exam Topic 4)

What process entails taking sensitive data and removing the indirect identifiers from each data object so that the identification of a single entity would not be possible?

- A. Tokenization
- B. Encryption
- C. Anonymization
- D. Masking

Answer: C

Explanation:

Anonymization is a type of masking, where indirect identifiers are removed from a data set to prevent the mapping back of data to an individual. Although masking refers to the overall approach of covering sensitive data, anonymization is the best answer here because it is more specific to exactly what is being asked. Tokenization involves the replacement of sensitive data with a key value that can be matched back to the real value. However, it is not focused on indirect identifiers or preventing the matching to an individual. Encryption refers to the overall process of protecting data via key pairs and protecting confidentiality.

NEW QUESTION 99

- (Exam Topic 4)

Which protocol operates at the network layer and provides for full point-to-point encryption of all communications and transmissions?

- A. IPSec
- B. VPN
- C. SSL
- D. TLS

Answer: A

Explanation:

IPSec is a protocol for encrypting and authenticating packets during transmission between two parties and can involve any type of device, application, or service. The protocol performs both the authentication and negotiation of security policies between the two parties at the start of the connection and then maintains these policies throughout the lifetime of the connection. TLS operates at the application layer, not the network layer, and is widely used to secure communications between two parties. SSL is similar to TLS but has been deprecated. Although a VPN allows a secure channel for communications into a private network from an outside location, it's not a protocol.

NEW QUESTION 100

- (Exam Topic 4)

Maintenance mode requires all of these actions except:

- A. Remove all active production instances
- B. Ensure logging continues
- C. Initiate enhanced security controls
- D. Prevent new logins

Answer: C

Explanation:

While the other answers are all steps in moving from normal operations to maintenance mode, we do not necessarily initiate any enhanced security controls.

NEW QUESTION 103

- (Exam Topic 4)

User access to the cloud environment can be administered in all of the following ways except:

- A. Provider provides administration on behalf the customer
- B. Customer directly administers access
- C. Third party provides administration on behalf of the customer
- D. Customer provides administration on behalf of the provider

Answer: D

Explanation:

The customer does not administer on behalf of the provider. All the rest are possible options.

NEW QUESTION 106

- (Exam Topic 4)

BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business. Which concept pertains to the amount of data and services needed to reach the predetermined level of operations?

- A. SRE

- B. RPO
- C. RSL
- D. RTO

Answer: B

Explanation:

The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the predetermined level of operations necessary during a BCDR situation. The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. SRE is provided as an erroneous response.

NEW QUESTION 107

- (Exam Topic 4)

To address shared monitoring and testing responsibilities in a cloud configuration, the provider might offer all these to the cloud customer except:

- A. Access to audit logs and performance data
- B. DLP solution results
- C. Security control administration
- D. SIM, SEI
- E. and SEM logs

Answer: C

Explanation:

While the provider might share any of the other options listed, the provider will not share administration of security controls with the customer. Security controls are the sole province of the provider.

NEW QUESTION 109

- (Exam Topic 4)

What is the cloud service model in which the customer is responsible for administration of the OS?

- A. QaaS
- B. SaaS
- C. PaaS
- D. IaaS

Answer: D

Explanation:

In IaaS, the cloud provider only owns the hardware and supplies the utilities. The customer is responsible for the OS, programs, and data. In PaaS and SaaS, the provider also owns the OS. There is no QaaS. That is a red herring.

NEW QUESTION 111

- (Exam Topic 4)

Which of the following is the least challenging with regard to eDiscovery in the cloud?

- A. Identifying roles such as data owner, controller and processor
- B. Decentralization of data storage
- C. Forensic analysis
- D. Complexities of International law

Answer: C

Explanation:

Forensic analysis is the least challenging of the answers provided as it refers to the analysis of data once it is obtained. The challenges revolve around obtaining the data for analysis due to the complexities of international law, the decentralization of data storage or difficulty knowing where to look, and identifying the data owner, controller, and processor.

NEW QUESTION 115

- (Exam Topic 4)

What is the concept of isolating an application from the underlying operating system for testing purposes?

- A. Abstracting
- B. Application virtualization
- C. Hosting
- D. Sandboxing

Answer: B

Explanation:

Application virtualization is a software implementation that allows applications and programs to run in an isolated environment rather than directly interacting with the operating system. Sandboxing refers to segregating information or processes for security or testing purposes, but it's not directly related to isolation from the underlying operating system. Abstracting sounds similar to the correct term but is not pertinent to the question, and hosting is provided as an erroneous answer.

NEW QUESTION 117

- (Exam Topic 4)

Which component of ITIL involves the creation of an RFC ticket and obtaining official approvals for it?

- A. Problem management
- B. Release management
- C. Deployment management
- D. Change management

Answer: D

Explanation:

The change management process involves the creation of the official Request for Change (RFC) ticket, which is used to document the change, obtain the required approvals from management and stakeholders, and track the change to completion. Release management is a subcomponent of change management, where the actual code or configuration change is put into place. Deployment management is similar to release management, but it's where changes are actually implemented on systems. Problem management is focused on the identification and mitigation of known problems and deficiencies before they are able to occur.

NEW QUESTION 120

- (Exam Topic 4)

In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?

- A. HIPAA
- B. The contract
- C. Statutes
- D. Security control matrix

Answer: B

Explanation:

The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable. The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

NEW QUESTION 125

- (Exam Topic 4)

Whereas a contract articulates overall priorities and requirements for a business relationship, which artifact enumerates specific compliance requirements, metrics, and response times?

- A. Service level agreement
- B. Service level contract
- C. Service compliance contract
- D. Service level amendment

Answer: A

Explanation:

The service level agreement (SLA) articulates minimum requirements for uptime, availability, processes, customer service and support, security controls, auditing requirements, and any other key aspect or requirement of the contract. Although the other choices sound similar to the correct answer, none is the proper term for this concept.

NEW QUESTION 129

- (Exam Topic 4)

Which of the following is the primary purpose of an SOC 3 report?

- A. HIPAA compliance
- B. Absolute assurances
- C. Seal of approval
- D. Compliance with PCI/DSS

Answer: C

Explanation:

The SOC 3 report is more of an attestation than a full evaluation of controls associated with a service provider.

NEW QUESTION 131

- (Exam Topic 4)

Which of the following best describes a sandbox?

- A. An isolated space where untested code and experimentation can safely occur separate from the production environment.
- B. A space where you can safely execute malicious code to see what it does.
- C. An isolated space where transactions are protected from malicious software
- D. An isolated space where untested code and experimentation can safely occur within the production environment.

Answer: A

Explanation:

Options C and B are also correct, but A is more general and incorporates them both. D is incorrect, because sandboxing does not take place in the production environment.

NEW QUESTION 133

- (Exam Topic 4)

When using a SaaS solution, what is the capability provided to the customer?

- A. To use the provider's applications running on a cloud infrastructure
- B. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface
- C. The consumer does manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- D. To use the consumer's applications running on a cloud infrastructure
- E. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface
- F. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- G. To use the consumer's applications running on a cloud infrastructure
- H. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface
- I. The consumer does manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- J. To use the provider's applications running on a cloud infrastructure
- K. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface
- L. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Answer: D

Explanation:

According to "The NIST Definition of Cloud Computing," in SaaS, "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

NEW QUESTION 136

- (Exam Topic 4)

Which of the following is NOT one of the official risk rating categories?

- A. Critical
- B. Low
- C. Catastrophic
- D. Minimal

Answer: C

Explanation:

The official categories of cloud risk ratings are Minimal, Low, Moderate, High, and Critical.

NEW QUESTION 140

- (Exam Topic 3)

An SLA contains the official requirements for contract performance and satisfaction between the cloud provider and cloud customer. Which of the following would NOT be a component with measurable metrics and requirements as part of an SLA?

- A. Network
- B. Users
- C. Memory
- D. CPU

Answer: B

Explanation:

Dealing with users or user access would not be an appropriate item for inclusion in an SLA specifically. However, user access and user experience would be covered indirectly through other metrics. Memory, CPU, and network resources are all typically included within an SLA for availability and response times when dealing with any incidents.

NEW QUESTION 144

- (Exam Topic 3)

Which of the following systems is used to employ a variety of different techniques to discover and alert on threats and potential threats to systems and networks?

- A. IDS
- B. IPS
- C. Firewall
- D. WAF

Answer: A

Explanation:

An intrusion detection system (IDS) is implemented to watch network traffic and operations, using predefined criteria or signatures, and alert administrators if anything suspect is found. An intrusion prevention system (IPS) is similar to an IDS but actually takes action against suspect traffic, whereas an IDS just alerts when it finds anything suspect. A firewall works at the network level and only takes into account IP addresses, ports, and protocols; it does not inspect the traffic for patterns or content. A web application firewall (WAF) works at the application layer and provides additional security via proxying, filtering service requests, or

blocking based on additional factors such as the client and requests.

NEW QUESTION 145

- (Exam Topic 3)

Clustered systems can be used to ensure high availability and load balancing across individual systems through a variety of methodologies.

What process is used within a clustered system to ensure proper load balancing and to maintain the health of the overall system to provide high availability?

- A. Distributed clustering
- B. Distributed balancing
- C. Distributed optimization
- D. Distributed resource scheduling

Answer: D

Explanation:

Distributed resource scheduling (DRS) is used within all clustered systems as the method for providing high availability, scaling, management, workload distribution, and the balancing of jobs and processes. None of the other choices is the correct term in this case.

NEW QUESTION 150

- (Exam Topic 3)

Which cloud deployment model is MOST likely to offer free or very cheap services to users?

- A. Hybrid
- B. Community
- C. Public
- D. Private

Answer: C

Explanation:

Public clouds offer services to anyone, regardless of affiliation, and are the most likely to offer free services to users. Examples of public clouds with free services include iCloud, Dropbox, and OneDrive. Private cloud models are designed for specific customers and for their needs, and would not offer services to the public at large, for free or otherwise. A community cloud is specific to a group of similar organizations and would not offer free or widely available public services. A hybrid cloud model would not fit the specifics of the question.

NEW QUESTION 152

- (Exam Topic 3)

Jurisdictions have a broad range of privacy requirements pertaining to the handling of personal data and information.

Which jurisdiction requires all storage and processing of data that pertains to its citizens to be done on hardware that is physically located within its borders?

- A. Japan
- B. United States
- C. European Union
- D. Russia

Answer: D

Explanation:

The Russian government requires all data and processing of information about its citizens to be done solely on systems and applications that reside within the physical borders of the country. The United States, European Union, and Japan focus their data privacy laws on requirements and methods for the protection of data, rather than where the data physically resides.

NEW QUESTION 157

- (Exam Topic 3)

Where is an XML firewall most commonly and effectively deployed in the environment?

- A. Between the application and data layers
- B. Between the presentation and application layers
- C. Between the IPS and firewall
- D. Between the firewall and application server

Answer: D

Explanation:

An XML firewall is most commonly deployed in line between the firewall and application server to validate XML code before it reaches the application. An XML firewall is intended to validate XML before it reaches the application. Placing the XML firewall between the presentation and application layers, between the firewall and IPS, or between the application and data layers would not serve the intended purpose.

NEW QUESTION 159

- (Exam Topic 3)

During which phase of the cloud data lifecycle is it possible for the classification of data to change?

- A. Use
- B. Archive
- C. Create
- D. Share

Answer:

C

Explanation:

The create phase encompasses any time data is created, imported, or modified. With any change in the content or value of data, the classification may also change. It must be continually reevaluated to ensure proper security. During the use, share, and archive phases, the data is not modified in any way, so the original classification is still relevant.

NEW QUESTION 162

- (Exam Topic 3)

For service provisioning and support, what is the ideal amount of interaction between a cloud customer and cloud provider?

- A. Half
- B. Full
- C. Minimal
- D. Depends on the contract

Answer: C

Explanation:

The goal with any cloud-hosting setup is for the cloud customer to be able to perform most or all its functions for service provisioning and configuration without any need for support from or interaction with the cloud provider beyond the automated tools provided. To fulfill the tenants of on-demand self-service, required interaction with the cloud provider--either half time, full time, or a commensurate amount of time based on the contract--would be in opposition to a cloud's intended use. As such, these answers are incorrect.

NEW QUESTION 167

- (Exam Topic 3)

Although host-based and network-based IDSs perform similar functions and have similar capabilities, which of the following is an advantage of a network-based IDS over a host-based IDS, assuming all capabilities are equal?

- A. Segregated from host systems
- B. Network access
- C. Scalability
- D. External to system patching

Answer: A

Explanation:

A network-based IDS has the advantage of being segregated from host systems, and as such, it would not be open to compromise in the same manner a host-based system would be. Although a network-based IDS would be external to system patching, this is not the best answer here because it is a minor concern compared to segregation due to possible host compromise. Scalability is also not the best answer because, although a network-based IDS does remove processing from the host system, it is not a primary security concern. Network access is not a consideration because both a host-based IDS and a network-based IDS would have access to network resources.

NEW QUESTION 170

- (Exam Topic 3)

Within a federated identity system, which entity accepts tokens from the identity provider?

- A. Assertion manager
- B. Servicing party
- C. Proxy party
- D. Relying party

Answer: D

Explanation:

The relying party is attached to the application or service that a user is trying to access, and it accepts authentication tokens from the user's own identity provider in order to facilitate authentication and access. The other terms provided are all associated with federated systems, but none is the correct choice in this case.

NEW QUESTION 174

- (Exam Topic 3)

Audits are either done based on the status of a system or application at a specific time or done as a study over a period of time that takes into account changes and processes.

Which of the following pairs matches an audit type that is done over time, along with the minimum span of time necessary for it?

- A. SOC Type 2, one year
- B. SOC Type 1, one year
- C. SOC Type 2, one month
- D. SOC Type 2, six months

Answer: D

Explanation:

SOC Type 2 audits are done over a period of time, with six months being the minimum duration. SOC Type 1 audits are designed with a scope that's a static point in time, and the other times provided for SOC Type 2 are incorrect.

NEW QUESTION 178

- (Exam Topic 3)

Which of the following roles would be responsible for managing memberships in federations and the use and integration of federated services?

- A. Inter-cloud provider
- B. Cloud service business manager
- C. Cloud service administrator
- D. Cloud service integrator

Answer: A

Explanation:

The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated services. A cloud service administrator is responsible for testing, monitoring, and securing cloud services, as well as providing usage reporting and dealing with service problems. The cloud service integrator is responsible for connecting existing systems and services with a cloud. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

NEW QUESTION 181

- (Exam Topic 3)

In the wake of many scandals with major corporations involving fraud and the deception of investors and regulators, which of the following laws was passed to govern accounting and financial records and disclosures?

- A. GLBA
- B. Safe Harbor
- C. HIPAA
- D. SOX

Answer: D

Explanation:

The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and accounting errors. The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy. The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Safe Harbor program was designed by the US government as a way for American companies to comply with European Union privacy laws.

NEW QUESTION 186

- (Exam Topic 3)

Most APIs will support a variety of different data formats or structures. However, the SOAP API will only support which one of the following data formats?

- A. XML
- B. XSLT
- C. JSON
- D. SAML

Answer: A

Explanation:

The Simple Object Access Protocol (SOAP) protocol only supports the Extensible Markup Language (XML) data format. Although the other options are all data formats or data structures, they are not supported by SOAP.

NEW QUESTION 191

- (Exam Topic 3)

Which data state would be most likely to use TLS as a protection mechanism?

- A. Data in use
- B. Data at rest
- C. Archived
- D. Data in transit

Answer: D

Explanation:

TLS would be used with data in transit, when packets are exchanged between clients or services and sent across a network. During the data-in-use state, the data is already protected via a technology such as TLS as it is exchanged over the network and then relies on other technologies such as digital signatures for protection while being used. The data-at-rest state primarily uses encryption for stored file objects. Archived data would be the same as data at rest.

NEW QUESTION 194

- (Exam Topic 3)

There is a large gap between the privacy laws of the United States and those of the European Union. Bridging this gap is necessary for American companies to do business with European companies and in European markets in many situations, as the American companies are required to comply with the stricter requirements. Which US program was designed to help companies overcome these differences?

- A. SOX
- B. HIPAA
- C. GLBA
- D. Safe Harbor

Answer: D

Explanation:

The Safe Harbor regulations were developed by the Department of Commerce and are meant to serve as a way to bridge the gap between privacy regulations of the European Union and the United States. Due to the lack of adequate privacy laws and protection on the federal level in the US, European privacy regulations generally prohibit the exporting of PII from Europe to the United States. Participation in the Safe Harbor program is voluntary on the part of US organizations. These organizations must conform to specific requirements and policies that mirror those from the EU, thus possibly fulfilling the EU requirements for data sharing and export. This way, American businesses can be allowed to serve customers in the EU. The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy. The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and errors.

NEW QUESTION 195

- (Exam Topic 3)

Which one of the following threat types to applications and services involves the sending of requests that are invalid and manipulated through a user's client to execute commands on the application under the user's own credentials?

- A. Injection
- B. Missing function-level access control
- C. Cross-site scripting
- D. Cross-site request forgery

Answer: D

Explanation:

A cross-site request forgery (CSRF) attack forces a client that a user has used to authenticate to an application to send forged requests under the user's own credentials to execute commands and requests that the application thinks are coming from a trusted client and user. Although this type of attack cannot be used to steal data directly because the attacker has no way of seeing the results of the commands, it does open other ways to compromise an application. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries.

NEW QUESTION 196

- (Exam Topic 3)

In order to comply with regulatory requirements, which of the following secure erasure methods would be available to a cloud customer using volume storage within the IaaS service model?

- A. Demagnetizing
- B. Shredding
- C. Degaussing
- D. Cryptographic erasure

Answer: D

Explanation:

Cryptographic erasure is a secure method to destroy data by destroying the keys that were used to encrypt it. This method is universally available for volume storage on IaaS and is also extremely quick. Shredding, degaussing, and demagnetizing are all physically destructive methods that would not be permitted within a cloud environment using shared resources.

NEW QUESTION 197

- (Exam Topic 3)

Three central concepts define what type of data and information an organization is responsible for pertaining to eDiscovery. Which of the following are the three components that comprise required disclosure?

- A. Possession, ownership, control
- B. Ownership, use, creation
- C. Control, custody, use
- D. Possession, custody, control

Answer: D

Explanation:

Data that falls under the purview of an eDiscovery request is that which is in the possession, custody, or control of the organization. Although this is an easy concept in a traditional data center, it can be difficult to distinguish who actually possesses and controls the data in a cloud environment due to multitenancy and resource pooling. Although these options provide similar-sounding terms, they are ultimately incorrect.

NEW QUESTION 199

- (Exam Topic 3)

Many different common threats exist against web-exposed services and applications. One attack involves attempting to leverage input fields to execute queries in a nested fashion that is unintended by the developers.

What type of attack is this?

- A. Injection
- B. Missing function-level access control
- C. Cross-site scripting
- D. Cross-site request forgery

Answer: A

Explanation:

An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or

system execute the code as part of its normal processing and queries. This can trick an application into exposing data that is not intended or authorized to be exposed, or it can potentially allow an attacker to gain insight into configurations or security controls. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes.

NEW QUESTION 200

- (Exam Topic 3)

One of the main components of system audits is the ability to track changes over time and to match these changes with continued compliance and internal processes.

Which aspect of cloud computing makes this particular component more challenging than in a traditional data center?

- A. Portability
- B. Virtualization
- C. Elasticity
- D. Resource pooling

Answer: B

Explanation:

Cloud services make exclusive use of virtualization, and systems change over time, including the addition, subtraction, and reimaging of virtual machines. It is extremely unlikely that the exact same virtual machines and images used in a previous audit would still be in use or even available for a later audit, making the tracking of changes over time extremely difficult, or even impossible. Elasticity refers to the ability to add and remove resources from a system or service to meet current demand, and although it plays a factor in making the tracking of virtual machines very difficult over time, it is not the best answer in this case. Resource pooling pertains to a cloud environment sharing a large amount of resources between different customers and services. Portability refers to the ability to move systems or services easily between different cloud providers.

NEW QUESTION 202

- (Exam Topic 3)

With a cloud service category where the cloud customer is responsible for deploying all services, systems, and components needed for their applications, which of the following storage types are MOST likely to be available to them?

- A. Structured and hierarchical
- B. Volume and object
- C. Volume and database
- D. Structured and unstructured

Answer: B

Explanation:

The question is describing the Infrastructure as a Service (IaaS) cloud offering, and as such, the volume and object storage types will be available to the customer. Structured and unstructured are storage types associated with PaaS, and although the other answers present similar-sounding storage types, they are a mix of real and fake names.

NEW QUESTION 207

- (Exam Topic 3)

ISO/IEC has established international standards for many aspects of computing and any processes or procedures related to information technology. Which ISO/IEC standard has been established to provide a framework for handling eDiscovery processes?

- A. ISO/IEC 27001
- B. ISO/IEC 27002
- C. ISO/IEC 27040
- D. ISO/IEC 27050

Answer: D

Explanation:

ISO/IEC 27050 strives to establish an internationally accepted standard for eDiscovery processes and best practices. It encompasses all steps of the eDiscovery process, including the identification, preservation, collection, processing, review, analysis, and the final production of the requested data archive. ISO/IEC 27001 is a general security specification for an information security management system. ISO/IEC 27002 gives best practice recommendations for information security management. ISO/IEC 27040 is focused on the security of storage systems.

NEW QUESTION 208

- (Exam Topic 3)

Which of the following is NOT one of the main intended goals of a DLP solution?

- A. Showing due diligence
- B. Preventing malicious insiders
- C. Regulatory compliance
- D. Managing and minimizing risk

Answer: B

Explanation:

Data loss prevention (DLP) extends the capabilities for data protection beyond the standard and traditional security controls that are offered by operating systems, application containers, and network devices. DLP is not specifically implemented to counter malicious insiders, and would not be particularly effective in doing so, because a malicious insider with legitimate access would have other ways to obtain data. DLP is a set of practices and controls to manage and minimize risk, comply with regulatory requirements, and show due diligence with the protection of data.

NEW QUESTION 213

- (Exam Topic 3)

Implementing baselines on systems would take an enormous amount of time and resources if the staff had to apply them to each server, and over time, it would be almost impossible to keep all the systems in sync on an ongoing basis.

Which of the following is NOT a package that can be used for implementing and maintaining baselines across an enterprise?

- A. Puppet
- B. SCCM
- C. Chef
- D. GitHub

Answer: D

Explanation:

GitHub is a software development platform that serves as a code repository and versioning system. It is solely used for software development and would not be appropriate for applying baselines to systems. Puppet is an open-source configuration management tool that runs on many platforms and can be used to apply and maintain baselines. The Software Center Configuration Manager (SCCM) was developed by Microsoft for managing systems across large groups of servers. Chef is also a system for maintaining large groups of systems throughout an enterprise.

NEW QUESTION 218

- (Exam Topic 3)

Many tools and technologies are available for securing or monitoring data in transit within a data center, whether it is a traditional data center or a cloud.

Which of the following is NOT a technology for securing data in transit?

- A. VPN
- B. TLS
- C. DNSSEC
- D. HTTPS

Answer: C

Explanation:

DNSSEC is an extension of the normal DNS protocol that enables a system to verify the integrity of a DNS query resolution by signing it from the authoritative source and verifying the signing chain. It is not used for securing data transmissions or exchanges. HTTPS is the most common method for securing web service and data calls within a cloud, and TLS is the current standard for encrypting HTTPS traffic. VPNs are widely used for securing data transmissions and service access.

NEW QUESTION 223

- (Exam Topic 3)

Although the REST API supports a wide variety of data formats for communications and exchange, which data formats are the most commonly used?

- A. SAML and HTML
- B. XML and SAML
- C. XML and JSON
- D. JSON and SAML

Answer: C

Explanation:

JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API and are typically implemented with caching for increased scalability and performance. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data. HTML is used for authoring web pages for consumption by web browsers.

NEW QUESTION 228

- (Exam Topic 3)

The management plane is used to administer a cloud environment and perform administrative tasks across a variety of systems, but most specifically it's used with the hypervisors.

What does the management plane typically leverage for this orchestration?

- A. APIs
- B. Scripts
- C. TLS
- D. XML

Answer: A

Explanation:

The management plane uses APIs to execute remote calls across the cloud environment to various management systems, especially hypervisors. This allows a centralized administrative interface, often a web portal, to orchestrate tasks throughout an enterprise. Scripts may be utilized to execute API calls, but they are not used directly to interact with systems. XML is used for data encoding and transmission, but not for executing remote calls. TLS is used to encrypt communications and may be used with API calls, but it is not the actual process for executing commands.

NEW QUESTION 232

- (Exam Topic 3)

If you are running an application that has strict legal requirements that the data cannot reside on systems that contain other applications or systems, which aspect of cloud computing would be prohibitive in this case?

- A. Multitenancy

- B. Broad network access
- C. Portability
- D. Elasticity

Answer: A

Explanation:

Multitenancy is the aspect of cloud computing that involves having multiple customers and applications running within the same system and sharing the same resources. Although considerable mechanisms are in place to ensure isolation and separation, the data and applications are ultimately using shared resources. Broad network access refers to the ability to access cloud services from any location or client. Portability refers to the ability to easily move cloud services between different cloud providers, whereas elasticity refers to the capabilities of a cloud environment to add or remove services, as needed, to meet current demand.

NEW QUESTION 237

- (Exam Topic 3)

Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?

- A. Regulation
- B. Multitenancy
- C. Virtualization
- D. Resource pooling

Answer: B

Explanation:

With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers. Especially within a public cloud model, it is not possible or practical for a cloud provider to alter its services for specific customer demands. Resource pooling and virtualization within a cloud environment would be the same for all customers, and would not impact certifications that a cloud provider might be willing to pursue. Regulations would form the basis for certification problems and would be a reason for a cloud provider to pursue specific certifications to meet customer requirements.

NEW QUESTION 240

- (Exam Topic 2)

Which of the following is a widely used tool for code development, branching, and collaboration?

- A. GitHub
- B. Maestro
- C. Orchestrator
- D. Conductor

Answer: A

Explanation:

GitHub is an open source tool that developers leverage for code collaboration, branching, and versioning.

NEW QUESTION 245

- (Exam Topic 2)

Which of the cloud deployment models involves spanning multiple cloud environments or a mix of cloud hosting models?

- A. Community
- B. Public
- C. Hybrid
- D. Private

Answer: C

Explanation:

A hybrid cloud model involves the use of more than one type of cloud hosting models, typically the mix of private and public cloud hosting models.

NEW QUESTION 248

- (Exam Topic 2)

Which crucial aspect of cloud computing can be most threatened by insecure APIs?

- A. Automation
- B. Redundancy
- C. Resource pooling
- D. Elasticity

Answer: A

Explanation:

Cloud environments depend heavily on API calls for management and automation. Any vulnerability with the APIs can cause significant risk and exposure to all tenants of the cloud environment.

NEW QUESTION 251

- (Exam Topic 2)

Which aspect of cloud computing makes it very difficult to perform repeat audits over time to track changes and compliance?

- A. Virtualization
- B. Multitenancy
- C. Resource pooling
- D. Dynamic optimization

Answer: A

Explanation:

Cloud environments will regularly change virtual machines as patching and versions are changed. Unlike a physical environment, there is little continuity from one period of time to another. It is very unlikely that the same virtual machines would be in use during a repeat audit.

NEW QUESTION 252

- (Exam Topic 2)

Which of the following does NOT fall under the "IT" aspect of quality of service (QoS)?

- A. Applications
- B. Key performance indicators (KPIs)
- C. Services
- D. Security

Answer: B

Explanation:

KPIs fall under the "business" aspect of QoS, along with monitoring and measuring of events and business processes. Services, security, and applications are all core components and concepts of the "IT" aspect of QoS.

NEW QUESTION 255

- (Exam Topic 2)

Which aspect of security is DNSSEC designed to ensure?

- A. Integrity
- B. Authentication
- C. Availability
- D. Confidentiality

Answer: A

Explanation:

DNSSEC is a security extension to the regular DNS protocol and services that allows for the validation of the integrity of DNS lookups. It does not address confidentiality or availability at all. It allows for a DNS client to perform DNS lookups and validate both their origin and authority via the cryptographic signature that accompanies the DNS response.

NEW QUESTION 260

- (Exam Topic 2)

Which security concept, if implemented correctly, will protect the data on a system, even if a malicious actor gains access to the actual system?

- A. Sandboxing
- B. Encryption
- C. Firewalls
- D. Access control

Answer: B

Explanation:

In any environment, data encryption is incredibly important to prevent unauthorized exposure of data either internally or externally. If a system is compromised by an attack, having the data encrypted on the system will prevent its unauthorized exposure or export, even with the system itself being exposed.

NEW QUESTION 263

- (Exam Topic 2)

Which value refers to the amount of time it takes to recover operations in a BCDR situation to meet management's objectives?

- A. RSL
- B. RPO
- C. SRE
- D. RTO

Answer: D

Explanation:

The recovery time objective (RTO) is a measure of the amount of time it would take to recover operations in the event of a disaster to the point where management's objectives are met for BCDR.

NEW QUESTION 266

- (Exam Topic 2)

Which approach is typically the most efficient method to use for data discovery?

- A. Metadata

- B. Content analysis
- C. Labels
- D. ACLs

Answer: A

Explanation:

Metadata is data about data. It contains information about the type of data, how it is stored and organized, or information about its creation and use.

NEW QUESTION 268

- (Exam Topic 2)

Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?

- A. Platform
- B. Infrastructure
- C. Governance
- D. Application

Answer: C

Explanation:

Regardless of which cloud-hosting model is used, the cloud customer always has sole responsibility for the governance of systems and data.

NEW QUESTION 270

- (Exam Topic 2)

From a security perspective, which of the following is a major concern when evaluating possible BCDR solutions?

- A. Access provisioning
- B. Auditing
- C. Jurisdictions
- D. Authorization

Answer: C

Explanation:

When a security professional is considering cloud solutions for BCDR, a top concern is the jurisdiction where the cloud systems are hosted. If the jurisdiction is different from where the production systems are hosted, they may be subjected to different regulations and controls, which would make a seamless BCDR solution far more difficult.

NEW QUESTION 272

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the requirements placed on the cloud provider by the cloud customer for minimum performance standards and requirements that must be met?

- A. Regulatory requirements
- B. SLAs
- C. Auditability
- D. Governance

Answer: B

Explanation:

Whereas a contract spells out general terms and costs for services, the SLA is where the real meat of the business relationship and concrete requirements come into play. The SLA spells out in clear terms the minimum requirements for uptime, availability, processes, customer service and support, security controls and requirements, auditing and reporting, and potentially many other areas that define the business relationship and the success of it.

NEW QUESTION 273

- (Exam Topic 2)

Which type of controls are the SOC Type 1 reports specifically focused on?

- A. Integrity
- B. PII
- C. Financial
- D. Privacy

Answer: C

Explanation:

SOC Type 1 reports are focused specifically on internal controls as they relate to financial reporting.

NEW QUESTION 275

- (Exam Topic 2)

Other than cost savings realized due to measured service, what is another facet of cloud computing that will typically save substantial costs in time and money for an organization in the event of a disaster?

- A. Broad network access
- B. Interoperability

- C. Resource pooling
- D. Portability

Answer: A

Explanation:

With a typical BCDR solution, an organization would need some number of staff to quickly travel to the location of the BCDR site to configure systems and applications for recovery. With a cloud environment, everything is done over broad network access, with no need (or even possibility) to travel to a remote site at any time.

NEW QUESTION 277

- (Exam Topic 2)

Which security concept is based on preventing unauthorized access to data while also ensuring that it is accessible to those authorized to use it?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Nonrepudiation

Answer: C

Explanation:

The main goal of confidentiality is to ensure that sensitive information is not made available or leaked to parties that should not have access to it, while at the same time ensuring that those with appropriate need and authorization to access it can do so in a manner commensurate with their needs and confidentiality requirements.

NEW QUESTION 280

- (Exam Topic 2)

Which of the following service capabilities gives the cloud customer the most control over resources and configurations?

- A. Desktop
- B. Platform
- C. Infrastructure
- D. Software

Answer: C

Explanation:

The infrastructure service capability gives the cloud customer substantial control in provisioning and configuring resources, including processing, storage, and network resources.

NEW QUESTION 283

- (Exam Topic 2)

Which aspect of cloud computing would make the use of a cloud the most attractive as a BCDR solution?

- A. Interoperability
- B. Resource pooling
- C. Portability
- D. Measured service

Answer: D

Explanation:

Measured service means that costs are only incurred when a cloud customer is actually using cloud services. This is ideal for a business continuity and disaster recovery (BCDR) solution because it negates the need to keep hardware or resources on standby in case of a disaster. Services can be initiated when needed and without costs unless needed.

NEW QUESTION 287

- (Exam Topic 2)

At which stage of the BCDR plan creation phase should security be included in discussions?

- A. Define scope
- B. Analyze
- C. Assess risk
- D. Gather requirements

Answer: A

Explanation:

Security should be included in discussions from the very first phase when defining the scope. Adding security later is likely to incur additional costs in time and money, or will result in an incomplete or inadequate plan.

NEW QUESTION 289

- (Exam Topic 2)

What process is used within a clustered system to provide high availability and load balancing?

- A. Dynamic balancing

- B. Dynamic clustering
- C. Dynamic optimization
- D. Dynamic resource scheduling

Answer: D

Explanation:

Dynamic resource scheduling (DRS) is used within all clustering systems as the method for clusters to provide high availability, scaling, management, and workload distribution and balancing of jobs and processes. From a physical infrastructure perspective, DRS is used to balance compute loads between physical hosts in a cloud to maintain the desired thresholds and limits on the physical hosts.

NEW QUESTION 293

- (Exam Topic 2)

Which of the following can be useful for protecting cloud customers from a denial-of-service (DoS) attack against another customer hosted in the same cloud?

- A. Reservations
- B. Measured service
- C. Limits
- D. Shares

Answer: A

Explanation:

Reservations ensure that a minimum level of resources will always be available to a cloud customer for them to start and operate their services. In the event of a DoS attack against one customer, they can guarantee that the other customers will still be able to operate.

NEW QUESTION 295

- (Exam Topic 2)

Which of the following technologies is used to monitor network traffic and notify if any potential threats or attacks are noticed?

- A. IPS
- B. WAF
- C. Firewall
- D. IDS

Answer: D

Explanation:

An intrusion detection system (IDS) is designed to analyze network packets, compare their contents or characteristics against a set of configurations or signatures, and alert personnel if anything is detected that could constitute a threat or is otherwise designated for alerting.

NEW QUESTION 300

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the ability to reuse or move components of an application or service?

- A. Availability
- B. Interoperability
- C. Reversibility
- D. Portability

Answer: B

Explanation:

Interoperability is the ease with which one can move or reuse components of an application or service. This is maximized when services are designed without specific dependencies on underlying platforms, operating systems, locations, or cloud providers.

NEW QUESTION 304

- (Exam Topic 2)

What concept does the "R" represent with the DREAD model?

- A. Reproducibility
- B. Repudiation
- C. Risk
- D. Residual

Answer: A

Explanation:

Reproducibility is the measure of how easy it is to reproduce and successful use an exploit. Scoring within the DREAD model ranges from 0, signifying a nearly impossible exploit, up to 10, which signifies something that anyone from a simple function call could exploit, such as a URL.

NEW QUESTION 305

- (Exam Topic 2)

What is the concept of segregating information or processes, within the same system or application, for security reasons?

- A. fencing
- B. Sandboxing

- C. Cellblocking
- D. Pooling

Answer: B

Explanation:

Sandboxing involves segregating and isolating information or processes from others within the same system or application, typically for security concerns. This is generally used for data isolation (for example, keeping different communities and populations of users isolated from other similar data).

NEW QUESTION 306

- (Exam Topic 2)

Which of the following service capabilities gives the cloud customer the least amount of control over configurations and deployments?

- A. Platform
- B. Infrastructure
- C. Software
- D. Desktop

Answer: C

Explanation:

The software service capability gives the cloud customer a fully established application, where only minimal user configuration options are allowed.

NEW QUESTION 311

- (Exam Topic 2)

The European Union passed the first major regulation declaring data privacy to be a human right. In what year did it go into effect?

- A. 2010
- B. 2000
- C. 1995
- D. 1990

Answer: C

Explanation:

Adopted in 1995, Directive 95/46 EC establishes strong data protection and policy requirements, including the declaring of data privacy to be a human right. It establishes that an individual has the right to be notified when their personal data is being access or processed, that it only will ever be accessed for legitimate purposes, and that data will only be accessed to the exact extent it needs to be for the particular process or request.

NEW QUESTION 314

- (Exam Topic 1)

Which of the following roles is responsible for creating cloud components and the testing and validation of services?

- A. Cloud auditor
- B. Inter-cloud provider
- C. Cloud service broker
- D. Cloud service developer

Answer: D

Explanation:

The cloud service developer is responsible for developing and creating cloud components and services, as well as for testing and validating services.

NEW QUESTION 317

- (Exam Topic 1)

Which of the following roles is responsible for peering with other cloud services and providers?

- A. Cloud auditor
- B. Inter-cloud provider
- C. Cloud service broker
- D. Cloud service developer

Answer: B

Explanation:

The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated services.

NEW QUESTION 320

- (Exam Topic 1)

What are the two protocols that TLS uses?

- A. Handshake and record
- B. Transport and initiate
- C. Handshake and transport
- D. Record and transmit

Answer: A

Explanation:

TLS uses the handshake protocol to establish and negotiate the TLS connection, and it uses the record protocol for the secure transmission of data.

NEW QUESTION 323

- (Exam Topic 1)

What is the first stage of the cloud data lifecycle where security controls can be implemented?

- A. Use
- B. Store
- C. Share
- D. Create

Answer: B

Explanation:

The "store" phase of the cloud data lifecycle, which typically occurs simultaneously with the "create" phase, or immediately thereafter, is the first phase where security controls can be implemented. In most cases, the manner in which the data is stored will be based on its classification.

NEW QUESTION 325

- (Exam Topic 1)

Which of the following is NOT a criterion for data within the scope of eDiscovery?

- A. Possession
- B. Custody
- C. Control
- D. Archive

Answer: D

Explanation:

eDiscovery pertains to information and data that is in the possession, control, and custody of an organization.

NEW QUESTION 329

- (Exam Topic 1)

From a legal perspective, what is the most important first step after an eDiscovery order has been received by the cloud provider?

- A. Notification
- B. Key identification
- C. Data collection
- D. Virtual image snapshots

Answer: A

Explanation:

The contract should include requirements for notification by the cloud provider to the cloud customer upon the receipt of such an order. This serves a few important purposes. First, it keeps communication and trust open between the cloud provider and cloud customers. Second, and more importantly, it allows the cloud customer to potentially challenge the order if they feel they have the grounds or desire to do so.

NEW QUESTION 334

- (Exam Topic 1)

Within an Infrastructure as a Service model, which of the following would NOT be a measured service?

- A. CPU
- B. Storage
- C. Number of users
- D. Memory

Answer: C

Explanation:

Within IaaS, the number of users on a system is not relevant to the particular hosting model in regard to cloud resources. IaaS is focused on infrastructure needs of a system or application. Therefore, a factor such as the number of users that could affect licensing requirements, for example, would apply to the SaaS model, or in some instances to PaaS.

NEW QUESTION 337

- (Exam Topic 1)

Which of the following attempts to establish an international standard for eDiscovery processes and best practices?

- A. ISO/IEC 31000
- B. ISO/IEC 27050
- C. ISO/IEC 19888
- D. ISO/IEC 27001

Answer: B

Explanation:

ISO/IEC 27050 strives to establish an internationally accepted standard for eDiscovery processes and best practices. It encompasses all steps of the eDiscovery process: identification, preservation, collection, processing, review, analysis, and the final production of the requested data.

NEW QUESTION 340

- (Exam Topic 1)

What type of segregation and separation of resources is needed within a cloud environment for multitenancy purposes versus a traditional data center model?

- A. Virtual
- B. Security
- C. Physical
- D. Logical

Answer: D

Explanation:

Cloud environments lack the ability to physically separate resources like a traditional data center can. To compensate, cloud computing logical segregation concepts are employed. These include VLANs, sandboxing, and the use of virtual network devices such as firewalls.

NEW QUESTION 344

- (Exam Topic 1)

Which type of audit report does many cloud providers use to instill confidence in their policies, practices, and procedures to current and potential customers?

- A. SAS-70
- B. SOC 2
- C. SOC 1
- D. SOX

Answer: B

Explanation:

One approach that many cloud providers opt to take is to undergo a SOC 2 audit and make the report available to cloud customers and potential cloud customers as a way of providing security confidence without having to open their systems or sensitive information to the masses.

NEW QUESTION 349

- (Exam Topic 1)

Which United States law is focused on PII as it relates to the financial industry?

- A. HIPAA
- B. SOX
- C. Safe Harbor
- D. GLBA

Answer: D

Explanation:

The GLBA, as it is commonly called based on the lead sponsors and authors of the act, is officially known as "The Financial Modernization Act of 1999." It is specifically focused on PII as it relates to financial institutions. There are three specific components of it, covering various areas and use, on top of a general requirement that all financial institutions must provide all users and customers with a written copy of their privacy policies and practices, including with whom and for what reasons their information may be shared with other entities.

NEW QUESTION 351

- (Exam Topic 1)

If you're using iSCSI in a cloud environment, what must come from an external protocol or application?

- A. Kerberos support
- B. CHAP support
- C. Authentication
- D. Encryption

Answer: D

Explanation:

iSCSI does not natively support encryption, so another technology such as IPsec must be used to encrypt communications.

NEW QUESTION 353

- (Exam Topic 1)

Which of the following statements accurately describes VLANs?

- A. They are not restricted to the same data center or the same racks.
- B. They are not restricted to the name rack but restricted to the same data center.
- C. They are restricted to the same racks and data centers.
- D. They are not restricted to the same rack but restricted to same switches.

Answer: A

Explanation:

A virtual area network (VLAN) can span any networks within a data center, or it can span across different physical locations and data centers.

NEW QUESTION 355

- (Exam Topic 1)

Which of the following represents a control on the maximum amount of resources that a single customer, virtual machine, or application can consume within a cloud environment?

- A. Share
- B. Reservation
- C. Provision
- D. Limit

Answer: D

Explanation:

Limits are put in place to enforce a maximum on the amount of memory or processing a cloud customer can use. This can be done either on a virtual machine or as a comprehensive whole for a customer, and is meant to ensure that enormous cloud resources cannot be allocated or consumed by a single host or customer to the detriment of other hosts and customers.

NEW QUESTION 356

- (Exam Topic 1)

Which of the following is NOT a regulatory system from the United States federal government?

- A. PCI DSS
- B. FISMA
- C. SOX
- D. HIPAA

Answer: A

Explanation:

The payment card industry data security standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry regulatory standard, not a governmental one.

NEW QUESTION 361

- (Exam Topic 1)

Which of the following pertains to fire safety standards within a data center, specifically with their enormous electrical consumption?

- A. NFPA
- B. BICSI
- C. IDCA
- D. Uptime Institute

Answer: A

Explanation:

The standards put out by the National Fire Protection Association (NFPA) cover general fire protection best practices for any type of facility, but also specific publications pertaining to IT equipment and data centers.

NEW QUESTION 363

- (Exam Topic 1)

Which of the following represents a minimum guaranteed resource within a cloud environment for the cloud customer?

- A. Reservation
- B. Share
- C. Limit
- D. Provision

Answer: A

Explanation:

A reservation is a minimum resource that is guaranteed to a customer within a cloud environment. Within a cloud, a reservation can pertain to the two main aspects of computing: memory and processor. With a reservation in place, the cloud provider guarantees that a cloud customer will always have at minimum the necessary resources available to power on and operate any of their services.

NEW QUESTION 366

- (Exam Topic 1)

Which concept BEST describes the capability for a cloud environment to automatically scale a system or application, based on its current resource demands?

- A. On-demand self-service
- B. Resource pooling
- C. Measured service
- D. Rapid elasticity

Answer: D

Explanation:

Rapid elasticity allows a cloud environment to automatically add or remove resources to or from a system or application based on its current demands. Whereas a traditional data center model would require standby hardware and substantial effort to add resources in response to load increases, a cloud environment can easily and rapidly expand to meet resources demands, so long as the application is properly implemented for it.

NEW QUESTION 368

- (Exam Topic 1)

What is the primary reason that makes resolving jurisdictional conflicts complicated?

- A. Different technology standards
- B. Costs
- C. Language barriers
- D. Lack of international authority

Answer: D

Explanation:

With international operations, systems ultimately cross many jurisdictional boundaries, and many times, they conflict with each other. The major hurdle to overcome for an organization is the lack of an ultimate international authority to mediate such conflicts, with a likely result of legal efforts in each jurisdiction.

NEW QUESTION 369

- (Exam Topic 1)

Which of the following roles is responsible for gathering metrics on cloud services and managing cloud deployments and the deployment processes?

- A. Cloud service business manager
- B. Cloud service operations manager
- C. Cloud service manager
- D. Cloud service deployment manager

Answer: D

Explanation:

The cloud service deployment manager is responsible for gathering metrics on cloud services, managing cloud deployments and the deployment process, and defining the environments and processes.

NEW QUESTION 374

- (Exam Topic 1)

Which of the following would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?

- A. Resource pooling
- B. Virtualization
- C. Multitenancy
- D. Regulation

Answer: C

Explanation:

With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers, and especially within a public cloud model, it is not possible or practical for a cloud provider to alter their services for specific customer demands.

NEW QUESTION 377

- (Exam Topic 1)

Which of the following is considered an internal redundancy for a data center?

- A. Power distribution units
- B. Network circuits
- C. Power substations
- D. Generators

Answer: A

Explanation:

Power distribution units are internal to a data center and supply power to internal components such as racks, appliances, and cooling systems. As such, they are considered an internal redundancy.

NEW QUESTION 378

- (Exam Topic 1)

Which of the following concepts refers to a cloud customer paying only for the resources and offerings they use within a cloud environment, and only for the duration that they are consuming them?

- A. Consumable service
- B. Measured service
- C. Billable service
- D. Metered service

Answer: B

Explanation:

Measured service is where cloud services are delivered and billed in a metered way, where the cloud customer only pays for those that they actually use, and for the duration of time that they use them.

NEW QUESTION 379

- (Exam Topic 1)

Which of the following APIs are most commonly used within a cloud environment?

- A. REST and SAML
- B. SOAP and REST
- C. REST and XML
- D. XML and SAML

Answer: B

Explanation:

Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) are the most commonly used APIs within a cloud environment. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data.

NEW QUESTION 382

- (Exam Topic 1)

Which of the following threat types can occur when encryption is not properly applied or insecure transport mechanisms are used?

- A. Security misconfiguration
- B. Insecure direct object references
- C. Sensitive data exposure
- D. Unvalidated redirects and forwards

Answer: C

Explanation:

Sensitive data exposure occurs when information is not properly secured through encryption and secure transport mechanisms; it can quickly become an easy and broad method for attackers to compromise information. Web applications must enforce strong encryption and security controls on the application side, but secure methods of communications with browsers or other clients used to access the information are also required. Security misconfiguration occurs when applications and systems are not properly configured for security, often a result of misapplied or inadequate baselines. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, thus allowing spoofing for malware or phishing attacks.

NEW QUESTION 387

- (Exam Topic 1)

Which technology can be useful during the "share" phase of the cloud data lifecycle to continue to protect data as it leaves the original system and security controls?

- A. IPS
- B. WAF
- C. DLP
- D. IDS

Answer: C

Explanation:

Data loss prevention (DLP) can be applied to data that is leaving the security enclave to continue to enforce access restrictions and policies on other clients and systems.

NEW QUESTION 388

- (Exam Topic 1)

What is used for local, physical access to hardware within a data center?

- A. SSH
- B. KVM
- C. VPN
- D. RDP

Answer: B

Explanation:

Local, physical access in a data center is done via KVM (keyboard, video, mouse) switches.

NEW QUESTION 391

- (Exam Topic 1)

What must be secured on physical hardware to prevent unauthorized access to systems?

- A. BIOS
- B. SSH
- C. RDP

D. ALOM

Answer: A

Explanation:

BIOS is the firmware that governs the physical initiation and boot up of a piece of hardware. If it is compromised, an attacker could have access to hosted systems and make configurations changes to expose or disable some security elements on the system.

NEW QUESTION 392

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CCSP Practice Exam Features:

- * CCSP Questions and Answers Updated Frequently
- * CCSP Practice Questions Verified by Expert Senior Certified Staff
- * CCSP Most Realistic Questions that Guarantee you a Pass on Your First Try
- * CCSP Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CCSP Practice Test Here](#)