

ISC2

Exam Questions CCSP

Certified Cloud Security Professional



NEW QUESTION 1

- (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 required amount of time to restore services to the predetermined level?

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

Answer: C

Explanation:

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. 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. SRE is provided as an erroneous response.

NEW QUESTION 2

- (Exam Topic 4)

Countermeasures for protecting cloud operations against external attackers include all of the following except:

- A. Continual monitoring for anomalous activity.
- B. Detailed and extensive background checks.
- C. Regular and detailed configuration/change management activities
- D. Hardened devices and systems, including servers, hosts, hypervisors, and virtual machines.

Answer: B

Explanation:

Background checks are controls for attenuating potential threats from internal actors; external threats aren't likely to submit to background checks.

NEW QUESTION 3

- (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 4

- (Exam Topic 4)

Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?

- A. SOC 1
- B. SOC 2
- C. SOC 3
- D. SOC 4

Answer: B

Explanation:

SOC 2 deals with the CIA triad. SOC 1 is for financial reporting. SOC 3 is only an attestation by the auditor. There is no SOC 4.

NEW QUESTION 5

- (Exam Topic 4)

Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like:

- A. Ransomware
- B. Syn floods
- C. XSS and SQL injection
- D. Password cracking

Answer: C

Explanation:

WAFs detect how the application interacts with the environment, so they are optimal for detecting and refuting things like SQL injection and XSS. Password

cracking, syn floods, and ransomware usually aren't taking place in the same way as injection and XSS, and they are better addressed with controls at the router and through the use of HIDS, NIDS, and antimalware tools.

NEW QUESTION 6

- (Exam Topic 4)

A data custodian is responsible for which of the following?

- A. Data context
- B. Data content
- C. The safe custody, transport, storage of the data, and implementation of business rules
- D. Logging access and alerts

Answer: C

Explanation:

A data custodian is responsible for the safe custody, transport, and storage of data, and the implementation of business roles.

NEW QUESTION 7

- (Exam Topic 4)

Countermeasures for protecting cloud operations against internal threats include all of the following except:

- A. Extensive and comprehensive training programs, including initial, recurring, and refresher sessions
- B. Skills and knowledge testing
- C. Hardened perimeter devices
- D. Aggressive background checks

Answer: C

Explanation:

Hardened perimeter devices are more useful at attenuating the risk of external attack.

NEW QUESTION 8

- (Exam Topic 4)

Cloud systems are increasingly used for BCDR solutions for organizations. What aspect of cloud computing makes their use for BCDR the most attractive?

- A. On-demand self-service
- B. Measured service
- C. Portability
- D. Broad network access

Answer: B

Explanation:

Business continuity and disaster recovery (BCDR) solutions largely sit idle until they are actually needed. This traditionally has led to increased costs for an organization because physical hardware must be purchased and operational but is not used. By using a cloud system, an organization will only pay for systems when they are being used and only for the duration of use, thus eliminating the need for extra hardware and costs. Portability is the ability to easily move services among different cloud providers. Broad network access allows access to users and staff from anywhere and from different clients, and although this would be important for a BCDR situation, it is not the best answer in this case. On-demand self-service allows users to provision services automatically and when needed, and although this too would be important for BCDR situations, it is not the best answer because it does not address costs or the biggest benefits to an organization.

NEW QUESTION 9

- (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 10

- (Exam Topic 4)

What type of solution is at the core of virtually all directory services?

- A. WS
- B. LDAP
- C. ADFS
- D. PKI

Answer: B

Explanation:

The Lightweight Directory Access Protocol (LDAP) forms the basis of virtually all directory services, regardless of the specific vendor or software package. WS is a protocol for information exchange between two systems and does not actually store the data. ADFS is a Windows component for enabling single sign-on for the operating system and applications, but it relies on data from an LDAP server. PKI is used for managing and issuing security certificates.

NEW QUESTION 10

- (Exam Topic 4)

The WS-Security standards are built around all of the following standards except which one?

- A. SAML
- B. WDSL
- C. XML
- D. SOAP

Answer: A

Explanation:

The WS-Security specifications, as well as the WS-Federation system, are built upon XML, WDSL, and SOAP. SAML is a very similar protocol that is used as an alternative to WS.XML, WDSL, and SOAP are all integral to the WS-Security specifications.

NEW QUESTION 15

- (Exam Topic 4)

Which of the following frameworks focuses specifically on design implementation and management?

- A. ISO 31000:2009
- B. ISO 27017
- C. NIST 800-92
- D. HIPAA

Answer: A

Explanation:

ISO 31000:2009 specifically focuses on design implementation and management. HIPAA refers to health care regulations, NIST 800-92 is about log management, and ISO 27017 is about cloud specific security controls.

NEW QUESTION 17

- (Exam Topic 4)

What concept does the D represent within the STRIDE threat model?

- A. Denial of service
- B. Distributed
- C. Data breach
- D. Data loss

Answer: A

Explanation:

Any application can be a possible target of denial of service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for unauthenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks. None of the other options provided is the correct term.

NEW QUESTION 19

- (Exam Topic 4)

As a result of scandals involving publicly traded corporations such as Enron, WorldCom, and Adelphi, Congress passed legislation known as:

- A. SOX
- B. HIPAA
- C. FERPA
- D. GLBA

Answer: A

Explanation:

Sarbanes-Oxley was a direct response to corporate scandals. FERPA is related to education. GLBA is about the financial industry. HIPAA is about health care.

NEW QUESTION 20

- (Exam Topic 4)

All the following are data analytics modes, except:

- A. Datamining
- B. Agile business intelligence
- C. Refractory iterations
- D. Real-time analytics

Answer: C

Explanation:

All the others are data analytics methods, but “refractory iterations” is a nonsense term thrown in as a red herring.

NEW QUESTION 23

- (Exam Topic 4)

Which of the following jurisdictions lacks a comprehensive national policy on data privacy and the protection of personally identifiable information (PII)?

- A. European Union
- B. Asian-Pacific Economic Cooperation
- C. United States
- D. Russia

Answer: C

Explanation:

The United States has a myriad of regulations focused on specific types of data, such as healthcare and financial, but lacks an overall comprehensive privacy law on the national level. The European Union, the Asian-Pacific Economic Cooperation, and Russia all have national privacy protections and regulations for the handling the PII data of their citizens.

NEW QUESTION 24

- (Exam Topic 4)

The cloud customer’s trust in the cloud provider can be enhanced by all of the following except:

- A. SLAs
- B. Shared administration
- C. Audits
- D. real-time video surveillance

Answer: D

Explanation:

Video surveillance will not provide meaningful information and will not enhance trust. All the others will do it.

NEW QUESTION 27

- (Exam Topic 4)

IRM solutions allow an organization to place different restrictions on data usage than would otherwise be possible through traditional security controls. Which of the following controls would be possible with IRM that would not with traditional security controls?

- A. Copy
- B. Read
- C. Delete
- D. Print

Answer: D

Explanation:

Traditional security controls would not be able to restrict a user from printing something that they have the ability to access and read, but IRM solutions would allow for such a restriction. If a user has permissions to read a file, he can also copy the file or print it under traditional controls, and the ability to modify or write will give the user the ability to delete.

NEW QUESTION 32

- (Exam Topic 4)

Hardening the operating system refers to all of the following except:

- A. Limiting administrator access
- B. Closing unused ports
- C. Removing antimalware agents
- D. Removing unnecessary services and libraries

Answer: C

Explanation:

Removing antimalware agents. Hardening the operating system means making it more secure. Limiting administrator access, closing unused ports, and removing unnecessary services and libraries all have the potential to make an OS more secure. But removing antimalware agents would actually make the system less secure. If anything, antimalware agents should be added, not removed.

NEW QUESTION 33

- (Exam Topic 4)

What is the correct order of the phases of the data life cycle?

- A. Create, Use, Store, Share, Archive, Destroy
- B. Create, Archive, Store, Share, Use, Destroy
- C. Create, Store, Use, Archive, Share, Destroy
- D. Create, Store, Use, Share, Archive, Destroy

Answer: D

Explanation:

The other options are the names of the phases, but out of proper order.

NEW QUESTION 35

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 37

- (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 38

- (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 43

- (Exam Topic 4)

Your new CISO is placing increased importance and focus on regulatory compliance as your applications and systems move into cloud environments. Which of the following would NOT be a major focus of yours as you develop a project plan to focus on regulatory compliance?

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

Answer: D

Explanation:

The jurisdictions where data is being stored, processed, or consumed are the ones that dictate the regulatory frameworks and compliance requirements, regardless of who the data owner or custodian might be. The other concepts for protecting data would all play a prominent role in regulatory compliance with a move to the cloud environment. Each concept needs to be evaluated based on the new configurations as well as any potential changes in jurisdiction or requirements introduced with the move to a cloud.

NEW QUESTION 46

- (Exam Topic 4)

Data labels could include all the following, except:

- A. Multifactor authentication
- B. Access restrictions
- C. Confidentiality level
- D. Distribution limitations

Answer: A

Explanation:

All the others might be included in data labels, but multifactor authentication is a procedure used for access control, not a label.

NEW QUESTION 47

- (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 49

- (Exam Topic 4)

A localized incident or disaster can be addressed in a cost-effective manner by using which of the following?

- A. UPS
- B. Generators
- C. Joint operating agreements
- D. Strict adherence to applicable regulations

Answer: C

Explanation:

Joint operating agreements can provide nearby relocation sites so that a disruption limited to the organization's own facility and campus can be addressed at a different facility and campus. UPS and generators are not limited to serving needs for localized causes. Regulations do not promote cost savings and are not often the immediate concern during BC/DR activities.

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 56

- (Exam Topic 4)

The goals of DLP solution implementation include all of the following, except:

- A. Elasticity
- B. Policy enforcement
- C. Data discovery
- D. Loss of mitigation

Answer: A

Explanation:

DLP does not have anything to do with elasticity, which is the capability of the environment to scale up or down according to demand. All the rest are goals of DLP implementations.

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 61

- (Exam Topic 4)

Above and beyond general regulations for data privacy and protection, certain types of data are subjected to more rigorous regulations and oversight. Which of the following is not a regulatory framework for more sensitive or specialized data?

- A. FIPS 140-2
- B. FedRAMP
- C. PCI DSS
- D. HIPAA

Answer: A

Explanation:

The FIPS 140-2 standard pertains to the certification of cryptographic modules and is not a regulatory framework. The Payment Card Industry Data Security Standard (PCI DSS), the Federal Risk and Authorization Management Program (FedRAMP), and the Health Insurance Portability and Accountability Act (HIPAA) are all regulatory frameworks for sensitive or specialized data.

NEW QUESTION 62

- (Exam Topic 4)

When a system needs to be exposed to the public Internet, what type of secure system would be used to perform only the desired operations?

- A. Firewall
- B. Proxy
- C. Honeypot
- D. Bastion

Answer: D

Explanation:

A bastion is a system that is exposed to the public Internet to perform a specific function, but it is highly restricted and secured to just that function. Any nonessential services and access are removed from the bastion so that security countermeasures and monitoring can be focused just on the bastion's specific duties. A honeypot is a system designed to look like a production system to entice attackers, but it does not contain any real data. It is used for learning about types of attacks and enabling countermeasures for them. A firewall is used within a network to limit access between IP addresses and ports. A proxy server provides additional security to and rulesets for network traffic that is allowed to pass through it to a service destination.

NEW QUESTION 63

- (Exam Topic 4)

What is the experimental technology that might lead to the possibility of processing encrypted data without having to decrypt it first?

- A. AES
- B. Link encryption
- C. One-time pads
- D. Homomorphic encryption

Answer: D

Explanation:

AES is an encryption standard. Link encryption is a method for protecting communications traffic. One-time pads are an encryption method.

NEW QUESTION 68

- (Exam Topic 4)

Which protocol, as a part of TLS, handles negotiating and establishing a connection between two parties?

- A. Record
- B. Binding
- C. Negotiation
- D. Handshake

Answer: D

Explanation:

The TLS handshake protocol is what negotiates and establishes the TLS connection between two parties and enables a secure communications channel to then handle data transmissions. The TLS record protocol is the actual secure communications method for transmitting data; it's responsible for the encryption and authentication of packets throughout their transmission between the parties, and in some cases it also performs compression. Negotiation and binding are not protocols under TLS.

NEW QUESTION 73

- (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 74

- (Exam Topic 4)

What are third-party providers of IAM functions for the cloud environment?

- A. AESs
- B. SIEMs
- C. DLPs
- D. CASBs

Answer: D

Explanation:

Data loss, leak prevention, and protection is a family of tools used to reduce the possibility of unauthorized disclosure of sensitive information. SIEMs are tools used to collate and manage log data. AES is an encryption standard.

NEW QUESTION 76

- (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 78

- (Exam Topic 4)

Which of the following areas of responsibility would be shared between the cloud customer and cloud provider within the Software as a Service (SaaS) category?

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

Answer: C

Explanation:

With SaaS, the application is a shared responsibility between the cloud provider and cloud customer. Although the cloud provider is responsible for deploying, maintaining, and securing the application, the cloud customer does carry some responsibility for the configuration of users and options. Regardless of the cloud service category used, the physical environment is always the sole responsibility of the cloud provider. With all cloud service categories, the data and governance are always the sole responsibility of the cloud customer.

NEW QUESTION 82

- (Exam Topic 4)

Gathering business requirements can aid the organization in determining all of this information about organizational assets, except:

- A. Full inventory
- B. Criticality
- C. Value
- D. Usefulness

Answer: D

Explanation:

When we gather information about business requirements, we need to do a complete inventory, receive accurate valuation of assets (usually from the owners of those assets), and assess criticality; this collection of information does not tell us, objectively, how useful an asset is, however.

NEW QUESTION 87

- (Exam Topic 4)

Upon completing a risk analysis, a company has four different approaches to addressing risk. Which approach it takes will be based on costs, available options, and adherence to any regulatory requirements from independent audits.

Which of the following groupings correctly represents the four possible approaches?

- A. Accept, avoid, transfer, mitigate
- B. Accept, deny, transfer, mitigate
- C. Accept, deny, mitigate, revise
- D. Accept, dismiss, transfer, mitigate

Answer:

A

Explanation:

The four possible approaches to risk are as follows: accept (do not patch and continue with the risk), avoid (implement solutions to prevent the risk from occurring), transfer (take out insurance), and mitigate (change configurations or patch to resolve the risk). Each of these answers contains at least one incorrect approach name.

NEW QUESTION 90

- (Exam Topic 4)

The goals of SIEM solution implementation include all of the following, except:

- A. Dashboarding
- B. Performance enhancement
- C. Trend analysis
- D. Centralization of log streams

Answer: B

Explanation:

SIEM does not intend to provide any enhancement of performance; in fact, a SIEM solution may decrease performance because of additional overhead. All the rest are goals of SIEM implementations.

NEW QUESTION 91

- (Exam Topic 4)

Many aspects of cloud computing bring enormous benefits over a traditional data center, but also introduce new challenges unique to cloud computing. Which of the following aspects of cloud computing makes appropriate data classification of high importance?

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

Answer: A

Explanation:

With multitenancy, where different cloud customers all share the same physical systems and networks, data classification becomes even more important to ensure that the appropriate security controls are applied immediately to prevent any potential leakage or exposure to other customers. Portability refers to the ability to move easily from one cloud provider to another. Interoperability refers to the ability to reuse components and services for different uses. Reversibility refers to the ability of the cloud customer to quickly and completely remove all data and services from a cloud provider and to verify the removal.

NEW QUESTION 92

- (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 easy 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 96

- (Exam Topic 4)

For optimal security, trust zones are used for network segmentation and isolation. They allow for the separation of various systems and tiers, each with its own security level.

Which of the following is typically used to allow administrative personnel access to trust zones?

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

Answer: C

Explanation:

Virtual private networks (VPNs) are used to provide administrative personnel with secure communication channels through security systems and into trust zones. They allow staff who perform system administration tasks to have access to ports and systems that are not allowed from the public Internet. IPSec is an encryption protocol for point-to-point communications at the network level, and may be used within a trust zone but not to give access into a trust zone. TLS enables encryption of communications between systems and services and would likely be used to secure the VPN communications, but it does not represent the overall concept being asked for in the question. SSH allows for secure shell access to systems, but not for general access into trust zones.

NEW QUESTION 98

- (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 99

- (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 104

- (Exam Topic 4)

The various models generally available for cloud BC/DR activities include all of the following except:

- A. Private architecture, cloud backup
- B. Cloud provider, backup from another cloud provider
- C. Cloud provider, backup from same provider
- D. Cloud provider, backup from private provider

Answer: D

Explanation:

This is not a normal configuration and would not likely provide genuine benefit.

NEW QUESTION 107

- (Exam Topic 4)

What category of PII data can carry potential fines or even criminal charges for its improper use or disclosure?

- A. Protected
- B. Legal
- C. Regulated
- D. Contractual

Answer: C

Explanation:

Regulated PII data carries legal and jurisdictional requirements, along with official penalties for its misuse or disclosure, which can be either civil or criminal in nature. Legal and protected are similar terms, but neither is the correct answer in this case. Contractual requirements can carry financial or contractual impacts for the improper use or disclosure of PII data, but not legal or criminal penalties that are officially enforced.

NEW QUESTION 112

- (Exam Topic 4)

Which protocol, as a part of TLS, handles the actual secure communications and transmission of data?

- A. Negotiation
- B. Handshake
- C. Transfer
- D. Record

Answer: D

Explanation:

The TLS record protocol is the actual secure communications method for transmitting data; it's responsible for encrypting and authenticating packets throughout their transmission between the parties, and in some cases it also performs compression. The TLS handshake protocol is what negotiates and establishes the TLS connection between two parties and enables the secure communications channel to then handle data transmissions. Negotiation and transfer are not protocols under TLS.

NEW QUESTION 114

- (Exam Topic 4)

Which of the following best describes the purpose and scope of ISO/IEC 27034-1?

- A. Describes international privacy standards for cloud computing
- B. Serves as a newer replacement for NIST 800-52 r4
- C. Provides an overview of network and infrastructure security designed to secure cloud applications.
- D. Provides an overview of application security that introduces definitive concepts, principles, and processes involved in application security.

Answer: D

NEW QUESTION 115

- (Exam Topic 4)

In the cloud motif, the data owner is usually:

- A. The cloud provider
- B. In another jurisdiction
- C. The cloud customer
- D. The cloud access security broker

Answer: C

Explanation:

The data owner is usually considered the cloud customer in a cloud configuration; the data in question is the customer's information, being processed in the cloud. The cloud provider is only leasing services and hardware to the customer. The cloud access security broker (CASB) only handles access control on behalf of the cloud customer, and is not in direct contact with the production data.

NEW QUESTION 118

- (Exam Topic 4)

Which of the following is considered a technological control?

- A. Firewall software
- B. Firing personnel
- C. Fireproof safe
- D. Fire extinguisher

Answer: A

Explanation:

A firewall is a technological control. The safe and extinguisher are physical controls and firing someone is an administrative control.

NEW QUESTION 122

- (Exam Topic 4)

BCDR strategies do not typically involve the entire operations of an organization, but only those deemed critical to their business.

Which concept pertains to the amount of services that need to be recovered to meet BCDR objectives?

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

Answer: A

Explanation:

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

NEW QUESTION 127

- (Exam Topic 4)

What is the term we use to describe the general ease and efficiency of moving data from one cloud provider either to another cloud provider or down from the cloud?

- A. Obfuscation
- B. Elasticity
- C. Mobility
- D. Portability

Answer: D

Explanation:

Elasticity is the name for the benefit of cloud computing where resources can be apportioned as necessary to meet customer demand. Obfuscation is a technique to hide full raw datasets, either from personnel who do not have need to know or for use in testing. Mobility is not a term pertinent to the CBK.

NEW QUESTION 131

- (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 136

- (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 139

- (Exam Topic 4)

Which of the following is a valid risk management metric?

- A. KPI
- B. KRI
- C. SOC
- D. SLA

Answer: B

Explanation:

KRI stands for key risk indicator. KRIs are the red flags if you will in the world of risk management. When these change, they indicate something is amiss and should be looked at quickly to determine if the change is minor or indicative of something important.

NEW QUESTION 141

- (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 142

- (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 143

- (Exam Topic 3)

You are working for a cloud service provider and receive an eDiscovery order pertaining to one of your customers. Which of the following would be the most appropriate action to take first?

- A. Take a snapshot of the virtual machines
- B. Escrow the encryption keys
- C. Copy the data
- D. Notify the customer

Answer: D

Explanation:

When a cloud service provider receives an eDiscovery order pertaining to one of their customers, the first action they must take is to notify the customer. This allows the customer to be aware of what was received, as well as to conduct a review to determine if any challenges are necessary or warranted. Taking snapshots of virtual machines, copying data, and escrowing encryption keys are all processes involved in the actual collection of data and should not be performed until the customer has been notified of the request.

NEW QUESTION 145

- (Exam Topic 3)

Modern web service systems are designed for high availability and resiliency. Which concept pertains to the ability to detect problems within a system, environment, or application and programmatically invoke redundant systems or processes for mitigation?

- A. Elasticity
- B. Redundancy
- C. Fault tolerance
- D. Automation

Answer: C

Explanation:

Fault tolerance allows a system to continue functioning, even with degraded performance, if portions of it fail or degrade, without the entire system or service being taken down. It can detect problems within a service and invoke compensating systems or functions to keep functionality going. Although redundancy is similar to fault tolerance, it is more focused on having additional copies of systems available, either active or passive, that can take up services if one system goes down. Elasticity pertains to the ability of a system to resize to meet demands, but it is not focused on system failures. Automation, and its role in maintaining large systems with minimal intervention, is not directly related to fault tolerance.

NEW QUESTION 148

- (Exam Topic 3)

With finite resources available within a cloud, even the largest cloud providers will at times need to determine which customers will receive additional resources first.

What is the term associated with this determination?

- A. Weighting
- B. Prioritization
- C. Shares
- D. Scoring

Answer: C

Explanation:

Shares are used within a cloud environment to prioritize resource allocation when customer requests exceed the available resources. Cloud providers utilize shares by assigning a priority score to each customer and allocating resources to those with the highest scores first. Scoring is a component of shares that determines the actual order in which to allocate resources. Neither weighting nor prioritization is the correct term in this case.

NEW QUESTION 153

- (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 158

- (Exam Topic 3)

The president of your company has tasked you with implementing cloud services as the most efficient way of obtaining a robust disaster recovery configuration for your production services.

Which of the cloud deployment models would you MOST likely be exploring?

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

Answer: A

Explanation:

A hybrid cloud model spans two more different hosting configurations or cloud providers. This would enable an organization to continue using its current hosting configuration, while adding additional cloud services to enable disaster recovery capabilities. The other cloud deployment models--public, private, and community--would not be applicable for seeking a disaster recovery configuration where cloud services are to be leveraged for that purpose rather than production service hosting.

NEW QUESTION 160

- (Exam Topic 3)

A DLP solution/implementation has three main components. Which of the following is NOT one of the three main components?

- A. Monitoring
- B. Enforcement
- C. Auditing
- D. Discovery and classification

Answer: C

Explanation:

Auditing, which can be supported to varying degrees by DLP solutions, is not a core component of them. Data loss prevention (DLP) solutions have core components of discovery and classification, enforcement, and monitoring. Discovery and classification are concerned with determining which data should be applied to the DLP policies, and then determining its classification level. Monitoring is concerned with the actual watching of data and how it's used through its various stages. Enforcement is the actual application of policies determined from the discovery stage and then triggered during the monitoring stage.

NEW QUESTION 163

- (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 166

- (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 171

- (Exam Topic 3)

In order to prevent cloud customers from potentially consuming enormous amounts of resources within a cloud environment and thus having a negative impact on other customers, what concept is commonly used by a cloud provider?

- A. Limit
- B. Cap
- C. Throttle
- D. Reservation

Answer: A

Explanation:

A limit puts a maximum value on the amount of resources that may be consumed by either a system, a service, or a cloud customer. It is commonly used to

prevent one entity from consuming enormous amounts of resources and having an operational impact on other tenants within the same cloud system. Limits can either be hard or somewhat flexible, meaning a customer can borrow from other customers while still having their actual limit preserved. A reservation is a guarantee to a cloud customer that a certain level of resources will always be available to them, regardless of what operational demands are currently placed on the cloud environment. Both cap and throttle are terms that sound similar to limit, but they are not the correct terms in this case.

NEW QUESTION 173

- (Exam Topic 3)

If a company needed to guarantee through contract and SLAs that a cloud provider would always have available sufficient resources to start their services and provide a certain level of provisioning, what would the contract need to refer to?

- A. Limit
- B. Reservation
- C. Assurance
- D. Guarantee

Answer: B

Explanation:

A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources. A limit refers to the enforcement of a maximum level of resources that can be consumed by or allocated to a cloud customer, service, or system. Both guarantee and assurance are terms that sound similar to reservation, but they are not correct choices.

NEW QUESTION 174

- (Exam Topic 3)

Within an IaaS implementation, which of the following would NOT be a metric used to quantify service charges for the cloud customer?

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

Answer: B

Explanation:

Within IaaS, where the cloud customer is responsible for everything beyond the physical network, the number of users on a system would not be a factor in billing or service charges. The core cloud services for IaaS are based on the memory, storage, and CPU requirements of the cloud customer. Because the cloud customer with IaaS is responsible for its own images and deployments, these components comprise the basis of its cloud provisioning and measured services billing.

NEW QUESTION 175

4 to 80.6 degrees Fahrenheit (or 18 to 27 degrees Celsius) as the optimal temperature range for data centers. None of these options is the recommendation from ASHRAE.

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 176

- (Exam Topic 3)

The share phase of the cloud data lifecycle involves allowing data to leave the application, to be shared with external systems, services, or even other vendors/contractors.

What technology would be useful for protecting data at this point?

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

Answer: B

Explanation:

Data loss prevention (DLP) solutions allow for control of data outside of the application or original system. They can enforce granular control such as printing, copying, and being read by others, as well as forcing expiration of access. Intrusion detection system (IDS) and intrusion prevention system (IPS) solutions are used for detecting and blocking suspicious and malicious traffic, respectively, whereas a web application firewall (WAF) is used for enforcing security or other controls on web-based applications.

NEW QUESTION 177

- (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 181

- (Exam Topic 3)

Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.

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

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

Answer: D

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. The Sarbanes-Oxley Act (SOX) was passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders. The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

NEW QUESTION 182

- (Exam Topic 3)

Different certifications and standards take different approaches to data center design and operations. Although many traditional approaches use a tiered methodology, which of the following utilizes a macro-level approach to data center design?

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

Answer: A

Explanation:

The Infinity Paradigm of the International Data Center Authority (IDCA) takes a macro-level approach to data center design. The IDCA does not use a specific, focused approach on specific components to achieve tier status. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers.

NEW QUESTION 187

- (Exam Topic 3)

Many aspects and features of cloud computing can make eDiscovery compliance more difficult or costly. Which aspect of cloud computing would be the MOST complicating factor?

- A. Measured service
- B. Broad network access
- C. Multitenancy
- D. Portability

Answer: C

Explanation:

With multitenancy, multiple customers share the same physical hardware and systems. With the nature of a cloud environment and how it writes data across diverse systems that are shared by others, the process of eDiscovery becomes much more complicated. Administrators cannot pull physical drives or easily isolate which data to capture. They not only have to focus on which data they need to collect, while ensuring they find all of it, but they also have to make sure that other data is not accidentally collected and exposed along with it. Measured service is the aspect of a cloud where customers only pay for the services they are actually using, and for the duration of their use. Portability refers to the ease with which an application or service can be moved among different cloud providers. Broad network access refers to the nature of cloud services being accessed via the public Internet, either with or without secure tunneling technologies. None of these concepts would pertain to eDiscovery.

NEW QUESTION 190

- (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 191

- (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 196

- (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 201

- (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 206

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 210

- (Exam Topic 2)

What process is used within a cloud environment to maintain resource balancing and ensure that resources are available where and when needed?

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

Answer: D

Explanation:

Dynamic optimization is the process through which the cloud environment is constantly maintained to ensure resources are available when and where needed, and that physical nodes do not become overloaded or near capacity, while others are underutilized.

NEW QUESTION 213

- (Exam Topic 2)

What concept does the "T" represent in the STRIDE threat model?

- A. TLS
- B. Testing
- C. Tampering with data
- D. Transport

Answer: C

Explanation:

Any application that sends data to the user will face the potential that the user could manipulate or alter the data, whether it resides in cookies, GET or POST commands, or headers, or manipulates client-side validations. If the user receives data from the application, it is crucial that the application validate and verify any data that is received back from the user.

NEW QUESTION 217

- (Exam Topic 2)

Which of the cloud deployment models requires the cloud customer to be part of a specific group or organization in order to host cloud services within it?

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

Answer: A

Explanation:

A community cloud model is where customers that share a certain common bond or group membership come together to offer cloud services to their members, focused on common goals and interests.

NEW QUESTION 221

- (Exam Topic 2)

Which of the following is a commonly used tool for maintaining system configurations?

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

Answer: C

Explanation:

Puppet is a commonly used tool for maintaining system configurations based on policies, and done so from a centralized authority.

NEW QUESTION 224

- (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 227

- (Exam Topic 2)

Which value refers to the percentage of production level restoration needed to meet BCDR objectives?

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

Answer: C

Explanation:

The recovery service level (RSL) is a percentage measure of the total typical production service level that needs to be restored to meet BCDR objectives in the case of a failure.

NEW QUESTION 232

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the assigning of jobs, tasks, and roles, as well as to ensuring they are successful and properly performed?

- A. Service-level agreements
- B. Governance
- C. Regulatory requirements
- D. Auditability

Answer: B

Explanation:

Governance at its core is the idea of assigning jobs, takes, roles, and responsibilities and ensuring they are satisfactory performed.

NEW QUESTION 234

- (Exam Topic 2)

What provides the information to an application to make decisions about the authorization level appropriate when granting access?

- A. User
- B. Relying party
- C. Federation
- D. Identity Provider

Answer: D

Explanation:

Upon successful user authentication, the identity provider gives information about the user to the relying party that it needs to make authorization decisions for granting access as well as the level of access needed.

NEW QUESTION 238

- (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 241

- (Exam Topic 2)

Which regulatory system pertains to the protection of healthcare data?

- A. HIPAA
- B. HAS
- C. HITECH
- D. HFCA

Answer: A

Explanation:

The Health Insurance Portability and Accountability Act (HIPAA) sets stringent requirements in the United States for the protection of healthcare records.

NEW QUESTION 244

- (Exam Topic 2)

How many additional DNS queries are needed when DNSSEC integrity checks are added?

- A. Three
- B. Zero
- C. One
- D. Two

Answer: B

Explanation:

DNSSEC does not require any additional DNS queries to be performed. The DNSSEC integrity checks and validations are all performed as part of the single DNS lookup resolution.

NEW QUESTION 249

- (Exam Topic 2)

What type of security threat is DNSSEC designed to prevent?

- A. Account hijacking
- B. Snooping
- C. Spoofing
- D. Injection

Answer: C

Explanation:

DNSSEC is designed to prevent the spoofing and redirection of DNS resolutions to rogue sites.

NEW QUESTION 250

- (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 252

- (Exam Topic 2)

Which entity requires all collection and storing of data on their citizens to be done on hardware that resides within their borders?

- A. Russia
- B. France
- C. Germany
- D. United States

Answer: A

Explanation:

Signed into law and effective starting on September 1, 2015, Russian Law 526-FZ establishes that any collecting, storing, or processing of personal information or data on Russian citizens must be done from systems and databases that are physically located with the Russian Federation.

NEW QUESTION 253

- (Exam Topic 2)

What strategy involves replacing sensitive data with opaque values, usually with a means of mapping it back to the original value?

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

Answer: C

Explanation:

Tokenization is the practice of utilizing a random and opaque "token" value in data to replace what otherwise would be a sensitive or protected data object. The token value is usually generated by the application with a means to map it back to the actual real value, and then the token value is placed in the data set with the same formatting and requirements of the actual real value so that the application can continue to function without different modifications or code changes.

NEW QUESTION 256

- (Exam Topic 2)

What must SOAP rely on for security?

- A. Encryption
- B. Tokenization
- C. TLS
- D. SSL

Answer: A

Explanation:

Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for passing data, and it must rely on the encryption of those data packages for security.

NEW QUESTION 257

- (Exam Topic 2)

What does the REST API use to protect data transmissions?

- A. NetBIOS
- B. VPN

- C. Encapsulation
- D. TLS

Answer: D

Explanation:

Representational State Transfer (REST) uses TLS for communication over secured channels. Although REST also supports SSL, at this point SSL has been phased out due to vulnerabilities and has been replaced by TLS.

NEW QUESTION 261

- (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 262

- (Exam Topic 2)

Which of the following is a restriction that can be enforced by information rights management (IRM) that is not possible for traditional file system controls?

- A. Delete
- B. Modify
- C. Read
- D. Print

Answer: D

Explanation:

IRM allows an organization to control who can print a set of information. This is not possible under traditional file system controls, where if a user can read a file, they are able to print it as well.

NEW QUESTION 265

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the ability for a cloud customer to easily remove their applications and data from a cloud environment?

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

Answer: A

Explanation:

Reversibility is the ability for a cloud customer to easily remove their applications or data from a cloud environment, as well as to ensure that all traces of their applications or data have been securely removed per a predefined agreement with the cloud provider.

NEW QUESTION 266

- (Exam Topic 2)

Which type of testing uses the same strategies and toolsets that hackers would use?

- A. Penetration
- B. Dynamic
- C. Static
- D. Malicious

Answer: A

Explanation:

Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discover potential vulnerabilities.

NEW QUESTION 269

- (Exam Topic 1)

Which of the following would NOT be considered part of resource pooling with an Infrastructure as a Service implementation?

- A. Storage
- B. Application
- C. Memory
- D. CPU

Answer: B

Explanation:

Infrastructure as a Service pools the compute resources for platforms and applications to build upon, including CPU, memory, and storage. Applications are not part of an IaaS offering from the cloud provider.

NEW QUESTION 272

- (Exam Topic 1)

When is a virtual machine susceptible to attacks while a physical server in the same state would not be?

- A. When it is behind a WAF
- B. When it is behind an IPS
- C. When it is not patched
- D. When it is powered off

Answer: D

Explanation:

A virtual machine is ultimately an image file residing in a file system. Because of this, even when a virtual machine is "powered off," it is still susceptible to attacks and modification. A physical server that is powered off would not be susceptible to attacks.

NEW QUESTION 277

- (Exam Topic 1)

Which aspect of archiving must be tested regularly for the duration of retention requirements?

- A. Availability
- B. Recoverability
- C. Auditability
- D. Portability

Answer: B

Explanation:

In order for any archiving system to be deemed useful and compliant, regular tests must be performed to ensure the data can still be recovered and accessible, should it ever be needed, for the duration of the retention requirements.

NEW QUESTION 280

- (Exam Topic 1)

Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?

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

Answer: B

Explanation:

Popular services such as iCloud, Dropbox, and OneDrive are all publicly available and are open to any user for free, with possible add-on services offered for a cost.

NEW QUESTION 285

- (Exam Topic 1)

Which of the following actions will NOT make data part of the "create" phase of the cloud data lifecycle?

- A. Modifying metadata
- B. Importing data
- C. Modifying data
- D. Constructing new data

Answer: A

Explanation:

Although the initial phase is called "create," it can also refer to modification. In essence, any time data is considered "new," it is in the create phase. This can come from data that is newly created, data that is imported into a system and is new to that system, or data that is already present and modified into a new form or value. Modifying the metadata does not change the actual data.

NEW QUESTION 286

- (Exam Topic 1)

Which protocol allows a system to use block-level storage as if it was a SAN, but over TCP network traffic instead?

- A. SATA
- B. iSCSI
- C. TLS
- D. SCSI

Answer: B

Explanation:

iSCSI is a protocol that allows for the transmission and use of SCSI commands and features over a TCP-based network. iSCSI allows systems to use block-level storage that looks and behaves as a SAN would with physical servers, but to leverage the TCP network within a virtualized environment and cloud.

NEW QUESTION 291

- (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 294

- (Exam Topic 1)

Which of the following is the optimal temperature for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?

- A. 69.8-86.0degF (21-30degC)
- B. 64.4-80.6degF(18-27degC)
- C. 51.8-66.2degF(11-19degC)
- D. 44.6-60-8degF(7-16degC)

Answer: B

Explanation:

The guidelines from ASHRAE establish 64.4-80.6degF (18-27degC) as the optimal temperature for a data center.

NEW QUESTION 298

- (Exam Topic 1)

Which of the following approaches would NOT be considered sufficient to meet the requirements of secure data destruction within a cloud environment?

- A. Cryptographic erasure
- B. Zeroing
- C. Overwriting
- D. Deletion

Answer: D

Explanation:

Deletion merely removes the pointers to data on a system; it does nothing to actually remove and sanitize the data. As such, the data remains in a recoverable state, and more secure methods are needed to ensure it has been destroyed and is not recoverable by another party.

NEW QUESTION 301

- (Exam Topic 1)

Which technology is NOT commonly used for security with data in transit?

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

Answer: A

Explanation:

DNSSEC relates to the integrity of DNS resolutions and the prevention of spoofing or redirection, and does not pertain to the actual security of transmissions or the protection of data.

NEW QUESTION 305

- (Exam Topic 1)

Which United States program was designed to enable organizations to bridge the gap between privacy laws and requirements of the United States and the European Union?

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

Answer: C

Explanation:

Due to the lack of an adequate privacy law or protection at the federal level in the United States, European privacy regulations generally prohibit the exporting or

sharing of PII from Europe with the United States. Participation in the Safe Harbor program is voluntary on behalf of an organization, but it does require them to conform to specific requirements and policies that mirror those from the EU. Thus, organizations can fulfill requirements for data sharing and export and possibly serve customers in the EU.

NEW QUESTION 306

- (Exam Topic 1)

Which jurisdiction lacks specific and comprehensive privacy laws at a national or top level of legal authority?

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

Answer: D

Explanation:

The United States lacks a single comprehensive law at the federal level addressing data security and privacy, but there are multiple federal laws that deal with different industries.

NEW QUESTION 307

- (Exam Topic 1)

Which of the following roles is responsible for obtaining new customers and securing contracts and agreements?

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

Answer: B

Explanation:

The cloud service broker is responsible for obtaining new customers, analyzing the marketplace, and securing contracts and agreements.

NEW QUESTION 308

- (Exam Topic 1)

Which protocol does the REST API depend on?

- A. HTTP
- B. XML
- C. SAML
- D. SSH

Answer: A

Explanation:

Representational State Transfer (REST) is a software architectural scheme that applies the components, connectors, and data conduits for many web applications used on the Internet. It uses and relies on the HTTP protocol and supports a variety of data formats.

NEW QUESTION 311

- (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 316

- (Exam Topic 1)

Which of the following security measures done at the network layer in a traditional data center are also applicable to a cloud environment?

- A. Dedicated switches
- B. Trust zones
- C. Redundant network circuits
- D. Direct connections

Answer: B

Explanation:

Trust zones can be implemented to separate systems or tiers along logical lines for great security and access controls. Each zone can then have its own security

controls and monitoring based on its particular needs.

NEW QUESTION 319

- (Exam Topic 1)

Which of the following are the storage types associated with IaaS?

- A. Volume and object
- B. Volume and label
- C. Volume and container
- D. Object and target

Answer: A

NEW QUESTION 324

- (Exam Topic 1)

Which of the following threat types involves the sending of untrusted data to a user's browser to be executed with their own credentials and access?

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

Answer: B

Explanation:

Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or where the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with the user's own access and permissions, allowing an attacker to redirect their web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access.

NEW QUESTION 327

- (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 329

.....

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](#)