

Exam Questions CCSP

Certified Cloud Security Professional

<https://www.2passeasy.com/dumps/CCSP/>



NEW QUESTION 1

- (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 2

- (Exam Topic 4)

Which of the following storage types is most closely associated with a database-type storage implementation?

- A. Object
- B. Unstructured
- C. Volume
- D. Structured

Answer: D

Explanation:

Structured storage involves organized and categorized data, which most closely resembles and operates like a database system would.

NEW QUESTION 3

- (Exam Topic 4)

In which cloud service model is the customer required to maintain the OS?

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

Answer: A

Explanation:

In IaaS, the service is bare metal, and the customer has to install the OS and the software; the customer then is responsible for maintaining that OS. In the other models, the provider installs and maintains the OS.

NEW QUESTION 4

- (Exam Topic 4)

When data discovery is undertaken, three main approaches or strategies are commonly used to determine what the type of data, its format, and composition are for the purposes of classification.

Which of the following is NOT one of the three main approaches to data discovery?

- A. Content analysis
- B. Hashing
- C. Labels
- D. Metadata

Answer: B

Explanation:

Hashing involves taking a block of data and, through the use of a one-way operation, producing a fixed-size value that can be used for comparison with other data. It is used primarily for protecting data and allowing for rapid comparison when matching data values such as passwords. Labels involve looking for header information or other categorizations of data to determine its type and possible classifications. Metadata involves looking at information attributes of the data, such as creator, application, type, and so on, in determining classification. Content analysis involves examining the actual data itself for its composition and classification level.

NEW QUESTION 5

- (Exam Topic 4)

Which ITIL component is an ongoing, iterative process of tracking all deployed and configured resources that an organization uses and depends on, whether they are hosted in a traditional data center or a cloud?

- A. Problem management
- B. Continuity management
- C. Availability management
- D. Configuration management

Answer: D

Explanation:

Configuration management tracks and maintains detailed information about all IT components within an organization. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION 6

- (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 7

- (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 8

- (Exam Topic 4)

Which of the following is not a way to manage risk?

- A. Transferring
- B. Accepting
- C. Mitigating
- D. Enveloping

Answer: D

Explanation:

Enveloping is a nonsense term, unrelated to risk management. The rest are not.

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)

A variety of security systems can be integrated within a network--some that just monitor for threats and issue alerts, and others that take action based on signatures, behavior, and other types of rules to actively stop potential threats.

Which of the following types of technologies is best described here?

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

Answer: B

Explanation:

An intrusion prevention system (IPS) can inspect traffic and detect any suspicious traffic based on a variety of factors, but it can also actively block such traffic. Although an IDS can detect the same types of suspicious traffic as an IPS, it is only design to alert, not to block. A firewall is only concerned with IP addresses, ports, and protocols; it cannot be used for the signature-based detection of traffic. A proxy can limit or direct traffic based on more extensive factors than a network firewall can, but it's not capable of using the same signature detection rules as an IPS.

NEW QUESTION 12

- (Exam Topic 4)

In addition to battery backup, a UPS can offer which capability?

- A. Breach alert
- B. Confidentiality
- C. Communication redundancy
- D. Line conditioning

Answer: D

Explanation:

A UPS can provide line conditioning, adjusting power so that it is optimized for the devices it serves and smoothing any power fluctuations; it does not offer any of the other listed functions.

NEW QUESTION 15

- (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 19

- (Exam Topic 4)

Which of the following best describes a cloud carrier?

- A. The intermediary who provides connectivity and transport of cloud providers and cloud consumers
- B. A person or entity responsible for making a cloud service available to consumers
- C. The person or entity responsible for transporting data across the Internet
- D. The person or entity responsible for keeping cloud services running for customers

Answer: A

Explanation:

A cloud carrier is the intermediary who provides connectivity and transport of cloud services between cloud providers and cloud customers.

NEW QUESTION 22

- (Exam Topic 4)

Which of the following is NOT a component of access control?

- A. Accounting

- B. Federation
- C. Authorization
- D. Authentication

Answer: B

Explanation:

Federation is not a component of access control. Instead, it is used to allow users possessing credentials from other authorities and systems to access services outside of their domain. This allows for access and trust without the need to create additional, local credentials. Access control encompasses not only the key concepts of authorization and authentication, but also accounting. Accounting consists of collecting and maintaining logs for both authentication and authorization for operational and regulatory requirements.

NEW QUESTION 25

- (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 28

- (Exam Topic 4)

What is the intellectual property protection for the tangible expression of a creative idea?

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

Answer: B

Explanation:

Copyrights are protected tangible expressions of creative works. The other answers listed are answers to subsequent questions.

NEW QUESTION 30

- (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 33

- (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 36

- (Exam Topic 4)

Database activity monitoring (DAM) can be:

- A. Host-based or network-based
- B. Server-based or client-based
- C. Used in the place of encryption
- D. Used in place of data masking

Answer: A

Explanation:

We don't use DAM in place of encryption or masking; DAM augments these options without replacing them. We don't usually think of the database interaction as client-server, so A is the best answer.

NEW QUESTION 37

- (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 41

- (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 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 42

- (Exam Topic 4)

Deviations from the baseline should be investigated and _____.

- A. Revealed
- B. Documented
- C. Encouraged
- D. Enforced

Answer: B

Explanation:

All deviations from the baseline should be documented, including details of the investigation and outcome. We do not enforce or encourage deviations. Presumably, we would already be aware of the deviation, so "revealing" is not a reasonable answer.

NEW QUESTION 46

- (Exam Topic 4)

An audit scope statement defines the limits and outcomes from an audit.

Which of the following would NOT be included as part of an audit scope statement?

- A. Reports
- B. Certification
- C. Billing
- D. Exclusions

Answer: C

Explanation:

Billing for an audit, or other cost-related items, would not be part of an audit scope statement and would instead be handled prior to the actual audit as part of the contract between the organization and auditors. Reports, exclusions to the scope of the audit, and required certifications on behalf of the systems or auditors are all crucial elements of an audit scope statement.

NEW QUESTION 48

- (Exam Topic 4)

Which of the following are attributes of cloud computing?

- A. Minimal management effort and shared resources
- B. High cost and unique resources
- C. Rapid provisioning and slow release of resources
- D. Limited access and service provider interaction

Answer: A

Explanation:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NEW QUESTION 50

- (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 55

- (Exam Topic 4)

Which component of ITIL involves planning for the restoration of services after an unexpected outage or incident?

- A. Continuity management
- B. Problem management
- C. Configuration management
- D. Availability management

Answer: A

Explanation:

Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Configuration management tracks and maintains detailed information about all IT components within an organization.

NEW QUESTION 60

- (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 64

- (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 68

- (Exam Topic 4)

All of the following are terms used to described 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 69

- (Exam Topic 4)

Data labels could include all the following, except:

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

Answer: B

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 70

- (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 73

- (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 74

- (Exam Topic 4)

The GAPP framework was developed through a joint effort between the major Canadian and American professional accounting associations in order to assist their members with managing and preventing risks to the privacy of their data and customers. Which of the following is the meaning of GAPP?

- A. General accounting personal privacy
- B. Generally accepted privacy practices
- C. Generally accepted privacy principles
- D. General accounting privacy policies

Answer: C

NEW QUESTION 76

- (Exam Topic 4)

When an organization is considering a cloud environment for hosting BCDR solutions, which of the following would be the greatest concern?

- A. Self-service
- B. Resource pooling
- C. Availability
- D. Location

Answer: D

Explanation:

If an organization wants to use a cloud service for BCDR, the location of the cloud hosting becomes a very important security consideration due to regulations and jurisdiction, which could be dramatically different from the organization's normal hosting locations. Availability is a hallmark of any cloud service provider, and likely

will not be a prime consideration when an organization is considering using a cloud for BCDR; the same goes for self-service options. Resource pooling is common among all cloud systems and would not be a concern when an organization is dealing with the provisioning of resources during a disaster.

NEW QUESTION 80

- (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 81

- (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 85

- (Exam Topic 4)

Which of the following report is most aligned with financial control audits?

- A. SSAE 16
- B. SOC 2
- C. SOC 1
- D. SOC 3

Answer: C

Explanation:

The SOC 1 report focuses primarily on controls associated with financial services. While IT controls are certainly part of most accounting systems today, the focus is on the controls around those financial systems.

NEW QUESTION 88

- (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 90

- (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 94

- (Exam Topic 4)

For performance purposes, OS monitoring should include all of the following except:

- A. Disk space
- B. Disk I/O usage
- C. CPU usage
- D. Print spooling

Answer: D

Explanation:

Print spooling is not a metric for system performance; all the rest are.

NEW QUESTION 98

- (Exam Topic 4)

Which of the following are cloud computing roles?

- A. Cloud service broker and user
- B. Cloud customer and financial auditor
- C. CSP and backup service provider
- D. Cloud service auditor and object

Answer: C

Explanation:

The following groups form the key roles and functions associated with cloud computing. They do not constitute an exhaustive list but highlight the main roles and functions within cloud computing:

- Cloud customer: An individual or entity that utilizes or subscribes to cloud based services or resources.
- CSP: A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations or individuals, usually for a fee; otherwise known to clients "as a service."
- Cloud backup service provider: A third-party entity that manages and holds operational responsibilities for cloud-based data backup services and solutions to customers from a central data center.
- CSB: Typically a third-party entity or company that looks to extend or enhance value to multiple customers of cloud-based services through relationships with multiple CSPs. It acts as a liaison between cloud services customers and CSPs, selecting the best provider for each customer and monitoring the services. The CSB can be utilized as a "middleman" to broker the best deal and customize services to the customer's requirements. May also resell cloud services.
- Cloud service auditor: Third-party organization that verifies attainment of SLAs.

NEW QUESTION 100

- (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 105

- (Exam Topic 4)

Which of the following methods of addressing risk is most associated with insurance?

- A. Mitigation
- B. Transference
- C. Avoidance
- D. Acceptance

Answer: B

Explanation:

Avoidance halts the business process, mitigation entails using controls to reduce risk, acceptance involves taking on the risk, and transference usually involves insurance.

NEW QUESTION 110

- (Exam Topic 4)

Which of the following is NOT considered a type of data loss?

- A. Data corruption
- B. Stolen by hackers
- C. Accidental deletion
- D. Lost or destroyed encryption keys

Answer: B

Explanation:

The exposure of data by hackers is considered a data breach. Data loss focuses on the data availability rather than security. Data loss occurs when data becomes lost, unavailable, or destroyed, when it should not have been.

NEW QUESTION 114

- (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 116

- (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 117

- (Exam Topic 4)

Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:

- A. The cloud provider's utilities
- B. The cloud provider's suppliers
- C. The cloud provider's resellers
- D. The cloud provider's vendors

Answer: C

Explanation:

The cloud provider's resellers are a marketing and sales mechanism, not an operational dependency that could affect the security of a cloud customer.

NEW QUESTION 118

- (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 122

- (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 124

- (Exam Topic 4)

On large distributed systems with pooled resources, cloud computing relies on extensive orchestration to maintain the environment and the constant provisioning of resources.

Which of the following is crucial to the orchestration and automation of networking resources within a cloud?

- A. DNSSEC
- B. DNS
- C. DCOM
- D. DHCP

Answer: D

Explanation:

The Dynamic Host Configuration Protocol (DHCP) automatically configures network settings for a host so that these settings do not need to be configured on the host statically. Given the rapid and programmatic provisioning of resources within a cloud environment, this capability is crucial to cloud operations. Both DNS and its security-integrity extension DNSSEC provide name resolution to IP addresses, but neither is used for the configuration of network settings on a host. DCOM refers to the Distributed Component Object Model, which was developed by Microsoft as a means to request services across a network, and is not used for network configurations at all.

NEW QUESTION 126

- (Exam Topic 4)

What concept and operational process must be spelled out clearly, as far as roles and responsibilities go, between the cloud provider and cloud customer for the mitigation of any problems or security events?

- A. Incident response
- B. Problem management
- C. Change management
- D. Conflict response

Answer: A

Explanation:

Incident response is the process through which security or operational issues are handled, including and coordination with and communication to the appropriate stakeholders. None of the other terms provided is the correct response.

NEW QUESTION 129

- (Exam Topic 4)

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

- A. Power failure
- B. Performance
- C. Bad policy
- D. Malicious disclosure

Answer: D

Explanation:

DLP tools can identify outbound traffic that violates the organization's policies. DLP will not protect against losses due to performance issues or power failures. The DLP solution must be configured according to the organization's policies, so bad policies will attenuate the effectiveness of DLP tools, not the other way around.

NEW QUESTION 134

- (Exam Topic 4)

Security is a critical yet often overlooked consideration for BCDR planning. At which stage of the planning process should security be involved?

- A. Scope definition
- B. Requirements gathering
- C. Analysis
- D. Risk assessment

Answer: A

Explanation:

Defining the scope of the plan is the very first step in the overall process. Security should be included from the very earliest stages and throughout the entire process. Bringing in security at a later stage can lead to additional costs and time delays to compensate for gaps in planning. Risk assessment, requirements gathering, and analysis are all later steps in the process, and adding in security at any of those points can potentially cause increased costs and time delays.

NEW QUESTION 139

- (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 144

- (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 145

- (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 150

- (Exam Topic 4)

Which of the following terms is not associated with cloud forensics?

- A. eDiscovery
- B. Chain of custody
- C. Analysis
- D. Plausibility

Answer: D

Explanation:

Plausibility, here, is a distractor and not specifically relevant to cloud forensics.

NEW QUESTION 151

- (Exam Topic 4)

When using an IaaS solution, what is the capability provided to the customer?

- A. To provision processing, storage, networks, and other fundamental computing resources when the consumer is able to deploy and run arbitrary software, which can include OSs and applications.
- B. To provision processing, storage, networks, and other fundamental computing resources when the auditor is able to deploy and run arbitrary software, which can include OSs and applications.
- C. To provision processing, storage, networks, and other fundamental computing resources when the provider is able to deploy and run arbitrary software, which can include OSs and applications.
- D. To provision processing, storage, networks, and other fundamental computing resources when the consumer is not able to deploy and run arbitrary software, which can include OSs and applications.

Answer: A

Explanation:

According to "The NIST Definition of Cloud Computing," in IaaS, "the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly

limited control of select networking components (e.g., host firewalls).

NEW QUESTION 152

- (Exam Topic 4)

Without the extensive funds of a large corporation, a small-sized company could gain considerable and cost-effective services for which of the following concepts by moving to a cloud environment?

- A. Regulatory
- B. Security
- C. Testing
- D. Development

Answer: B

Explanation:

Cloud environments, regardless of the specific deployment model used, have extensive and robust security controls in place, especially in regard to physical and infrastructure security. A small company can leverage the extensive security controls and monitoring provided by a cloud provider, which they would unlikely ever be able to afford on their own. Moving to a cloud would not result in any gains for development and testing because these areas require the same rigor regardless of where deployment and hosting occur. Regulatory compliance in a cloud would not be a gain for an organization because it would likely result in additional oversight and auditing as well as require the organization to adapt to a new environment.

NEW QUESTION 155

- (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 156

- (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 160

- (Exam Topic 4)

Which ITIL component is focused on anticipating predictable problems and ensuring that configurations and operations are in place to prevent these problems from ever occurring?

- A. Availability management
- B. Continuity management
- C. Configuration management
- D. Problem management

Answer: D

Explanation:

Problem management is focused on identifying and mitigating known problems and deficiencies before they are able to occur, as well as on minimizing the impact of incidents that cannot be prevented. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Configuration management tracks and maintains detailed information about all IT components within an organization.

NEW QUESTION 161

- (Exam Topic 4)

Which of the following components are part of what a CCSP should review when looking at contracting with a cloud service provider?

- A. Redundant uplink grafts
- B. Background checks for the provider's personnel

- C. The physical layout of the datacenter
- D. Use of subcontractors

Answer: D

Explanation:

The use of subcontractors can add risk to the supply chain and should be considered; trusting the provider's management of their vendors and suppliers (including subcontractors) is important to trusting the provider. Conversely, the customer is not likely to be allowed to review the physical design of the datacenter (or, indeed, even know the exact location of the datacenter) or the personnel security specifics for the provider's staff. "Redundant uplink grafts" is a nonsense term used as a distractor.

NEW QUESTION 164

- (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 167

- (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 169

- (Exam Topic 4)

Just like the risk management process, the BCDR planning process has a defined sequence of steps and processes to follow to ensure the production of a comprehensive and successful plan.

Which of the following is the correct sequence of steps for a BCDR plan?

- A. Define scope, gather requirements, assess risk, implement
- B. Define scope, gather requirements, implement, assess risk
- C. Gather requirements, define scope, implement, assess risk
- D. Gather requirements, define scope, assess risk, implement

Answer: A

Explanation:

The correct sequence for a BCDR plan is to define the scope, gather requirements based on the scope, assess overall risk, and implement the plan. The other sequences provided are not in the correct order.

NEW QUESTION 173

- (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 177

- (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 181

- (Exam Topic 4)

When an organization is considering the use of cloud services for BCDR planning and solutions, which of the following cloud concepts would be the most important?

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

Answer: D

Explanation:

Portability is the ability for a service or system to easily move among different cloud providers. This is essential for using a cloud solution for BCDR because vendor lock-in would inhibit easily moving and setting up services in the event of a disaster, or it would necessitate a large number of configuration or component changes to implement. Interoperability, or the ability to reuse components for other services or systems, would not be an important factor for BCDR. Reversibility, or the ability to remove all data quickly and completely from a cloud environment, would be important at the end of a disaster, but would not be important during setup and deployment. Elasticity, or the ability to resize resources to meet current demand, would be very beneficial to a BCDR situation, but not as vital as portability.

NEW QUESTION 183

- (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 188

- (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 193

- (Exam Topic 4)

In the cloud motif, the data processor is usually:

- A. The cloud customer
- B. The cloud provider
- C. The cloud access security broker
- D. The party that assigns access rights

Answer: B

Explanation:

In legal terms, when “data processor” is defined, it refers to anyone who stores, handles, moves, or manipulates data on behalf of the data owner or controller. In the cloud computing realm, this is the cloud provider.

NEW QUESTION 197

- (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 199

- (Exam Topic 4)

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

- A. Mandatory vacation
- B. Least privilege
- C. Separation of duties
- D. Conflict of interest

Answer: D

Explanation:

Conflict of interest is a threat, not a control.

NEW QUESTION 201

- (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 204

- (Exam Topic 4)

Having a reservation in a cloud environment can ensure operations continue in the event of high utilization across the cloud.

Which of the following would NOT be a capability covered by reservations?

- A. Performing business operations
- B. Starting virtual machines
- C. Running applications
- D. Auto-scaling

Answer: D

Explanation:

A reservation will not guarantee auto-scaling is available because it involves the allocation of additional resources beyond what a cloud customer already has provisioned. Reservations will guarantee minimal resources are available to start virtual machines, run applications, and perform normal business operations.

NEW QUESTION 209

- (Exam Topic 4)

Which aspect of cloud computing serves as the biggest challenge to using DLP to protect data at rest?

- A. Portability
- B. Resource pooling
- C. Interoperability
- D. Reversibility

Answer: B

Explanation:

Resource pooling serves as the biggest challenge to using DLP solutions to protect data at rest because data is spread across large systems, which are also shared by many different clients. With the data always moving and being distributed, additional challenges for protection are created versus a physical and isolated storage system. Portability is the ability to easily move between different cloud providers, and interoperability is focused on the ability to reuse components or services. Reversibility pertains to the ability of a cloud customer to easily and completely remove their data and services from a cloud provider.

NEW QUESTION 213

- (Exam Topic 4)

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

- A. Cell blocking
- B. Sandboxing
- C. Pooling
- D. Fencing

Answer: B

Explanation:

Sandboxing involves the segregation and isolation of information or processes from other information or processes within the same system or application, typically for security concerns. Sandboxing is generally used for data isolation (for example, keeping different communities and populations of users isolated from others with similar data). In IT terminology, pooling typically means bringing together and consolidating resources or services, not segregating or separating them. Cell blocking and fencing are both erroneous terms.

NEW QUESTION 214

- (Exam Topic 4)

Which is the lowest level of the CSA STAR program?

- A. Attestation
- B. Self-assessment
- C. Hybridization
- D. Continuous monitoring

Answer: B

Explanation:

The lowest level is Level 1, which is self-assessment, Level 2 is an external third-party attestation, and Level 3 is a continuous-monitoring program. Hybridization does not exist as part of the CSA STAR program.

NEW QUESTION 217

- (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 219

- (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 224

- (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 229

- (Exam Topic 4)

A UPS should have enough power to last how long?

- A. One day
- B. 12 hours
- C. Long enough for graceful shutdown
- D. 10 minutes

Answer: C

NEW QUESTION 231

- (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 236

- (Exam Topic 3)

Which of the following aspects of security is solely the responsibility of the cloud provider?

- A. Regulatory compliance
- B. Physical security
- C. Operating system auditing
- D. Personal security of developers

Answer: B

Explanation:

Regardless of the particular cloud service used, physical security of hardware and facilities is always the sole responsibility of the cloud provider. The cloud provider may release information about their physical security policies and procedures to ensure any particular requirements of potential customers will meet their regulatory obligations. Personal security of developers and regulatory compliance are always the responsibility of the cloud customer. Responsibility for operating systems, and the auditing of them, will differ based on the cloud service category used.

NEW QUESTION 237

- (Exam Topic 3)

The European Union is often considered the world leader in regard to the privacy of personal data and has declared privacy to be a "human right."

In what year did the EU first assert this principle?

- A. 1995
- B. 2000
- C. 2010
- D. 1999

Answer: A

Explanation:

The EU passed Directive 95/46 EC in 1995, which established data privacy as a human right. The other years listed are incorrect.

NEW QUESTION 241

- (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 243

- (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 244

- (Exam Topic 3)

Which cloud service category would be most ideal for a cloud customer that is developing software to test its applications among multiple hosting providers to determine the best option for its needs?

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

Answer: B

Explanation:

Platform as a Service would allow software developers to quickly and easily deploy their applications among different hosting providers for testing and validation in order to determine the best option. Although IaaS would also be appropriate for hosting applications, it would require too much configuration of application servers and libraries in order to test code. Conversely, PaaS would provide a ready-to-use environment from the onset. DaaS would not be appropriate in any way for software developers to use to deploy applications. IaaS would not be appropriate in this scenario because it would require the developers to also deploy and maintain the operating system images or to contract with another firm to do so. SaaS, being a fully functional software platform, would not be appropriate for deploying applications into.

NEW QUESTION 249

- (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 254

- (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 256

- (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 258

- (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 259

- (Exam Topic 3)

Which cloud storage type is typically used to house virtual machine images that are used throughout the environment?

- A. Structured
- B. Unstructured
- C. Volume
- D. Object

Answer: D

Explanation:

Object storage is typically used to house virtual machine images because it is independent from other systems and is focused solely on storage. It is also the most appropriate for handling large individual files. Volume storage, because it is allocated to a specific host, would not be appropriate for the storing of virtual images. Structured and unstructured are storage types specific to PaaS and would not be used for storing items used throughout a cloud environment.

NEW QUESTION 261

- (Exam Topic 3)

Within a federated identity system, which of the following would you be MOST likely to use for sending information for consumption by a relying party?

- A. XML
- B. HTML
- C. WS-Federation
- D. SAML

Answer: D

Explanation:

The Security Assertion Markup Language (SAML) is the most widely used method for encoding and sending attributes and other information from an identity provider to a relying party. WS-Federation, which is used by Active Directory Federation Services (ADFS), is the second most used method for sending information to a relying party, but it is not a better choice than SAML. XML is similar to SAML in the way it encodes and labels data, but it does not have all of the required extensions that SAML does. HTML is not used within federated systems at all.

NEW QUESTION 264

- (Exam Topic 3)

Your boss has tasked your team with getting your legacy systems and applications connected with new cloud-based services that management has decided are crucial to customer service and offerings.

Which role would you be assuming under this directive?

- A. Cloud service administrator

- B. Cloud service user
- C. Cloud service integrator
- D. Cloud service business manager

Answer: C

Explanation:

The cloud service integrator role is responsible for connecting and integrating existing services and applications with cloud-based 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 user is someone who consumes cloud services. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

NEW QUESTION 266

- (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 268

- (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 271

- (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 272

- (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 276

- (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 279

- (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 281

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 282

- (Exam Topic 3)

From a security perspective, what component of a cloud computing infrastructure represents the biggest concern?

- A. Hypervisor
- B. Management plane
- C. Object storage
- D. Encryption

Answer: B

Explanation:

The management plane will have broad administrative access to all host systems throughout an environment; as such, it represents the most pressing security concerns. A compromise of the management plane can directly lead to compromises of any other systems within the environment. Although hypervisors represent a significant security concern to an environment because their compromise would expose any virtual systems hosted within them, the management plane is a better choice in this case because it controls multiple hypervisors. Encryption and object storage both represent lower-level security concerns.

NEW QUESTION 287

- (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 291

- (Exam Topic 3)

Which of the following threat types involves the sending of commands or arbitrary data through input fields in an application in an attempt to get that code executed as part of normal processing?

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

Answer: C

Explanation:

An injection attack is where a malicious actor will send 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 could 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 294

- (Exam Topic 3)

With IaaS, what is responsible for handling the security and control over the volume storage space?

- A. Management plane
- B. Operating system
- C. Application
- D. Hypervisor

Answer: B

Explanation:

Volume storage is allocated via a LUN to a system and then treated the same as any traditional storage. The operating system is responsible for formatting and securing volume storage as well as controlling all access to it. Applications, although they may use volume storage and have permissions to write to it, are not responsible for its formatting and security. Both a hypervisor and the management plane are outside of an individual system and are not responsible for managing the files and storage within that system.

NEW QUESTION 297

- (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 299

- (Exam Topic 3)

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

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

Answer: B

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 to see 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. 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. 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 301

- (Exam Topic 3)

When an API is being leveraged, it will encapsulate its data for transmission back to the requesting party or service. What is the data encapsulation used with the SOAP protocol referred to as?

- A. Packet
- B. Payload
- C. Object
- D. Envelope

Answer: D

Explanation:

Simple Object Access Protocol (SOAP) encapsulates its information in what is known as a SOAP envelope. It then leverages common communications protocols for transmission. Object is a type of cloud storage, but also a commonly used term with certain types of programming languages. Packet and payload are terms that sound similar to envelope but are not correct in this case.

NEW QUESTION 302

- (Exam Topic 3)

Digital investigations have adopted many of the same methodologies and protocols as other types of criminal or scientific inquiries. What term pertains to the application of scientific norms and protocols to digital investigations?

- A. Scientific
- B. Investigative
- C. Methodological
- D. Forensics

Answer: D

Explanation:

Forensics refers to the application of scientific methods and protocols to the investigation of crimes. Although forensics has traditionally been applied to well-known criminal proceedings and investigations, the term equally applies to digital investigations and methods. Although the other answers provide similar-sounding terms and ideas, none is the appropriate answer in this case.

NEW QUESTION 306

- (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 310

- (Exam Topic 3)

Different types of audits are intended for different audiences, such as internal, external, regulatory, and so on. Which of the following audits are considered "restricted use" versus being for a more broad audience?

- A. SOC Type 2
- B. SOC Type 1
- C. SOC Type 3
- D. SAS-70

Answer: B

Explanation:

SOC Type 1 reports are intended for restricted use, only to be seen by the actual service organization, its current clients, or its auditors. These reports are not intended for wider or public distribution. SAS-70 audit reports have been deprecated and are no longer in use, and both the SOC Type 2 and 3 reports are designed to expand upon the SOC Type 1 reports and are for broader audiences.

NEW QUESTION 311

- (Exam Topic 3)

A crucial decision any company must make is in regard to where it hosts the data systems it depends on. A debate exists as to whether it's best to lease space in a

data center or build your own data center--and now with cloud computing, whether to purchase resources within a cloud. What is the biggest advantage to leasing space in a data center versus procuring cloud services?

- A. Regulations
- B. Control
- C. Security
- D. Costs

Answer: B

Explanation:

When leasing space in a data center versus utilizing cloud services, a customer has a much greater control over its systems and services, from both the hardware/software perspective and the operational management perspective. Costs, regulations, and security are all prime considerations regardless of the hosting type selected. Although regulations will be the same in either hosting solution, in most instances, costs and security will be greater factors with leased space.

NEW QUESTION 314

- (Exam Topic 3)

You just hired an outside developer to modernize some applications with new web services and functionality. In order to implement a comprehensive test platform for validation, the developer needs a data set that resembles a production data set in both size and composition. In order to accomplish this, what type of masking would you use?

- A. Development
- B. Replicated
- C. Static
- D. Dynamic

Answer: C

Explanation:

Static masking takes a data set and produces a copy of it, but with sensitive data fields masked. This allows for a full data set from production for testing purposes, but without any sensitive data. Dynamic masking works with a live system and is not used to produce a distinct copy. The terms "replicated" and "development" are not types of masking.

NEW QUESTION 318

- (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 322

- (Exam Topic 3)

With an API, various features and optimizations are highly desirable to scalability, reliability, and security. What does the REST API support that the SOAP API does NOT support?

- A. Acceleration
- B. Caching
- C. Redundancy
- D. Encryption

Answer: B

Explanation:

The Simple Object Access Protocol (SOAP) does not support caching, whereas the Representational State Transfer (REST) API does. The other options are all capabilities that are either not supported by SOAP or not supported by any API and must be provided by external features.

NEW QUESTION 326

- (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 330

- (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 333

- (Exam Topic 3)

Configurations and policies for a system can come from a variety of sources and take a variety of formats. Which concept pertains to the application of a set of configurations and policies that is applied to all systems or a class of systems?

- A. Hardening
- B. Leveling
- C. Baselines
- D. Standards

Answer: C

Explanation:

Baselines are a set of configurations and policies applied to all new systems or services, and they serve as the basis for deploying any other services on top of them. Although standards often form the basis for baselines, the term is applicable in this case. Hardening is the process of securing a system, often through the application of baselines. Leveling is an extraneous but similar term to baselining.

NEW QUESTION 336

- (Exam Topic 3)

Which aspect of SaaS will alleviate much of the time and energy organizations spend on compliance (specifically baselines)?

- A. Maintenance
- B. Licensing
- C. Standardization
- D. Development

Answer: C

Explanation:

With the entire software platform being controlled by the cloud provider, the standardization of configurations and versioning is done automatically for the cloud customer. This alleviates the customer's need to track upgrades and releases for its own systems and development; instead, the onus is on the cloud provider. Although licensing is the responsibility of the cloud customer within SaaS, it does not have an impact on compliance requirements. Within SaaS, development and maintenance of the system are solely the responsibility of the cloud provider.

NEW QUESTION 341

- (Exam Topic 3)

Which cloud storage type resembles a virtual hard drive and can be utilized in the same manner and with the same type of features and capabilities?

- A. Volume
- B. Unstructured
- C. Structured
- D. Object

Answer: A

Explanation:

Volume storage is allocated and mounted as a virtual hard drive within IaaS implementations, and it can be maintained and used the same way a traditional file system can. Object storage uses a flat structure on remote services that is accessed via opaque descriptors, structured storage resembles database storage, and unstructured storage is used to hold auxiliary files in conjunction with applications hosted within a PaaS implementation.

NEW QUESTION 343

- (Exam Topic 3)

Which phase of the cloud data lifecycle represents the first instance where security controls can be implemented?

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

Answer: C

Explanation:

The store phase occurs immediately after the create phase, and as data is committed to storage structures, the first opportunity for security controls to be implemented is realized. During the create phase, the data is not yet part of a system where security controls can be applied, and although the use and share phases also entail the application of security controls, they are not the first phase where the process occurs.

NEW QUESTION 347

- (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 351

- (Exam Topic 2)

Which OSI layer does IPsec operate at?

- A. Network
- B. transport
- C. Application
- D. Presentation

Answer: A

Explanation:

A major difference between IPsec and other protocols such as TLS is that IPsec operates at the Internet network layer rather than the application layer, allowing for complete end-to-end encryption of all communications and traffic.

NEW QUESTION 352

- (Exam Topic 2)

Which of the following is NOT a domain of the Cloud Controls Matrix (CCM)?

- A. Data center security
- B. Human resources
- C. Mobile security
- D. Budgetary and cost controls

Answer: D

Explanation:

Budgetary and cost controls is not one of the domains outlined in the CCM.

NEW QUESTION 353

- (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 358

- (Exam Topic 2)

What changes are necessary to application code in order to implement DNSSEC?

- A. Adding encryption modules
- B. Implementing certificate validations
- C. Additional DNS lookups
- D. No changes are needed.

Answer: D

Explanation:

To implement DNSSEC, no additional changes are needed to applications or their code because the integrity checks are all performed at the system level.

NEW QUESTION 361

- (Exam Topic 2)

What does the "SOC" acronym refer to with audit reports?

- A. Service Origin Confidentiality
- B. System Organization Confidentiality
- C. Service Organizational Control
- D. System Organization Control

Answer: C

NEW QUESTION 363

- (Exam Topic 2)

What concept does the "I" represent with the STRIDE threat model?

- A. Integrity
- B. Information disclosure
- C. IT security
- D. Insider threat

Answer: B

Explanation:

Perhaps the biggest concern for any user is having their personal and sensitive information disclosed by an application. There are many aspects of an application to consider with security and protecting this information, and it is very difficult for any application to fully ensure security from start to finish. The obvious focus is on security within the application itself, as well as protecting and storing the data.

NEW QUESTION 366

- (Exam Topic 2)

Which type of audit report is considered a "restricted use" report for its intended audience?

- A. SAS-70
- B. SSAE-16
- C. SOC Type 1
- D. SOC Type 2

Answer: C

Explanation:

SOC Type 1 reports are considered "restricted use" reports. They are intended for management and stakeholders of an organization, clients of the service organization, and auditors of the organization. They are not intended for release beyond those audiences.

NEW QUESTION 369

- (Exam Topic 2)

Which of the following is NOT a key area for performance monitoring as far as an SLA is concerned?

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

Answer: B

Explanation:

An SLA requires performance monitoring of CPU, memory, storage, and networking. The number of users active on a system would not be part of an SLA specifically, other than in regard to the impact on the other four variables.

NEW QUESTION 374

- (Exam Topic 2)

What does dynamic application security testing (DAST) NOT entail?

- A. Scanning
- B. Probing
- C. Discovery

D. Knowledge of the system

Answer: D

Explanation:

Dynamic application security testing (DAST) is considered "black box" testing and begins with no inside knowledge of the application or its configurations. Everything about the application must be discovered during the testing.

NEW QUESTION 375

- (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 377

- (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 380

- (Exam Topic 2)

Which of the following is NOT a function performed by the record protocol of TLS?

- A. Encryption
- B. Acceleration
- C. Authentication
- D. Compression

Answer: B

Explanation:

The record protocol of TLS performs the authentication and encryption of data packets, and in some cases compression as well. It does not perform any acceleration functions.

NEW QUESTION 382

- (Exam Topic 2)

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

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

Answer: D

Explanation:

XML firewalls are most commonly deployed in line between the firewall and application server to validate XML code before it reaches the application.

NEW QUESTION 385

- (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 388

- (Exam Topic 2)

Which audit type has been largely replaced by newer approaches since 2011?

- A. SOC Type 1
- B. SSAE-16
- C. SAS-70
- D. SOC Type 2

Answer: C

Explanation:

SAS-70 reports were replaced in 2011 with the SSAE-16 reports throughout the industry.

NEW QUESTION 390

- (Exam Topic 2)

With software-defined networking, what aspect of networking is abstracted from the forwarding of traffic?

- A. Routing
- B. Session
- C. Filtering
- D. Firewalling

Answer: C

Explanation:

With software-defined networking (SDN), the filtering of network traffic is separated from the forwarding of network traffic so that it can be independently administered.

NEW QUESTION 394

- (Exam Topic 2)

Which of the following is NOT an application or utility to apply and enforce baselines on a system?

- A. Chef
- B. GitHub
- C. Puppet
- D. Active Directory

Answer: B

Explanation:

GitHub is an application for code collaboration, including versioning and branching of code trees. It is not used for applying or maintaining system configurations.

NEW QUESTION 398

- (Exam Topic 2)

Which of the following service categories entails the least amount of support needed on the part of the cloud customer?

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

Answer: A

Explanation:

With SaaS providing a fully functioning application that is managed and maintained by the cloud provider, cloud customers incur the least amount of support responsibilities themselves of any service category.

NEW QUESTION 400

- (Exam Topic 2)

What concept does the "A" represent in the DREAD model?

- A. Affected users
- B. Authentication
- C. Affinity
- D. Authorization

Answer: A

Explanation:

Affected users refers to the percentage of users who would be impacted by a successful exploit. Scoring ranges from 0, which means no users are impacted, to 10, which means all users are impacted.

NEW QUESTION 405

- (Exam Topic 2)

What is a standard configuration and policy set that is applied to systems and virtual machines called?

- A. Standardization
- B. Baseline
- C. Hardening
- D. Redline

Answer: B

Explanation:

The most common and efficient manner of securing operating systems is through the use of baselines. A baseline is a standardized and understood set of base configurations and settings. When a new system is built or a new virtual machine is established, baselines will be applied to a new image to ensure the base configuration meets organizational policy and regulatory requirements.

NEW QUESTION 410

- (Exam Topic 2)

What is an often overlooked concept that is essential to protecting the confidentiality of data?

- A. Strong password
- B. Training
- C. Security controls
- D. Policies

Answer: B

Explanation:

While the main focus of confidentiality revolves around technological requirements or particular security methods, an important and often overlooked aspect of safeguarding data confidentiality is appropriate and comprehensive training for those with access to it. Training should be focused on the safe handling of sensitive information overall, including best practices for network activities as well as physical security of the devices or workstations used to access the application.

NEW QUESTION 414

- (Exam Topic 2)

What type of masking strategy involves replacing data on a system while it passes between the data and application layers?

- A. Dynamic
- B. Static
- C. Replication
- D. Duplication

Answer: A

Explanation:

With dynamic masking, production environments are protected with the masking process being implemented between the application and data layers of the application. This allows for a masking translation to take place live in the system and during normal application processing of data.

NEW QUESTION 415

- (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 416

- (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 418

- (Exam Topic 2)

Which of the following is the MOST important requirement and guidance for testing during an audit?

- A. Stakeholders
- B. Shareholders
- C. Management
- D. Regulations

Answer: D

Explanation:

During any audit, regulations are the most important factor and guidelines for what must be tested. Although the requirements from management, stakeholders, and shareholders are also important, regulations are not negotiable and pose the biggest risk to any organization for compliance failure.

NEW QUESTION 421

- (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 424

- (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 425

- (Exam Topic 2)

What type of data does data rights management (DRM) protect?

- A. Consumer
- B. PII
- C. Financial
- D. Healthcare

Answer: A

Explanation:

DRM applies to the protection of consumer media, such as music, publications, video, movies, and soon.

NEW QUESTION 428

- (Exam Topic 2)

Which of the following is NOT one of five principles of SOC Type 2 audits?

- A. Privacy
- B. Processing integrity
- C. Financial
- D. Security

Answer: C

Explanation:

The SOC Type 2 audits include five principles: security, privacy, processing integrity, availability, and confidentiality.

NEW QUESTION 431

- (Exam Topic 2)

Which of the following features is a main benefit of PaaS over IaaS?

- A. Location independence
- B. High-availability
- C. Physical security requirements
- D. Auto-scaling

Answer: D

Explanation:

With PaaS providing a fully configured and managed framework, auto-scaling can be implemented to programmatically adjust resources based on the current demands of the environment.

NEW QUESTION 433

- (Exam Topic 2)

What strategy involves hiding data in a data set to prevent someone from identifying specific individuals based on other data fields present?

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

Answer: A

Explanation:

With data anonymization, data is manipulated in such a way so as to prevent the identification of an individual through various data objects, and is often used in conjunction with other concepts such as masking.

NEW QUESTION 437

- (Exam Topic 2)

Which of the following service capabilities gives the cloud customer an established and maintained framework to deploy code and applications?

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

Answer: C

Explanation:

The platform service capability provides programming languages and libraries from the cloud provider, where the customer can deploy their own code and applications into a managed and controlled framework.

NEW QUESTION 441

- (Exam Topic 2)

Which of the following is NOT something that an HIDS will monitor?

- A. Configurations
- B. User logins
- C. Critical system files
- D. Network traffic

Answer: B

Explanation:

A host intrusion detection system (HIDS) monitors network traffic as well as critical system files and configurations.

NEW QUESTION 445

- (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 448

- (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 449

- (Exam Topic 2)

Which of the following is NOT a focus or consideration of an internal audit?

- A. Certification
- B. Design
- C. Costs
- D. Operational efficiency

Answer: A

Explanation:

In order to obtain and comply with certifications, independent external audits must be performed and satisfied. Although some testing of certification controls can be part of an internal audit, they will not satisfy requirements.

NEW QUESTION 454

- (Exam Topic 2)

Which aspect of cloud computing makes data classification even more vital than in a traditional data center?

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

Answer: C

Explanation:

With multiple tenants within the same hosting environment, any failure to properly classify data may lead to potential exposure to other customers and applications within the same environment.

NEW QUESTION 455

- (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 459

- (Exam Topic 1)

What does SDN stand for within a cloud environment?

- A. Software-dynamic networking
- B. Software-defined networking
- C. Software-dependent networking
- D. System-dynamic nodes

Answer: B

Explanation:

Software-defined networking separates the administration of network filtering and network forwarding to allow for distributed administration.

NEW QUESTION 460

- (Exam Topic 1)

What is the biggest concern with hosting a key management system outside of the cloud environment?

- A. Confidentiality
- B. Portability

- C. Availability
- D. Integrity

Answer: C

Explanation:

When a key management system is outside of the cloud environment hosting the application, availability is a primary concern because any access issues with the encryption keys will render the entire application unusable.

NEW QUESTION 461

- (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 466

- (Exam Topic 1)

Which of the following may unilaterally deem a cloud hosting model inappropriate for a system or application?

- A. Multitenancy
- B. Certification
- C. Regulation
- D. Virtualization

Answer: C

Explanation:

Some regulations may require specific security controls or certifications be used for hosting certain types of data or functions, and in some circumstances they may be requirements that are unable to be met by any cloud provider.

NEW QUESTION 467

- (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 472

- (Exam Topic 1)

Which publication from the United States National Institute of Standards and Technology pertains to defining cloud concepts and definitions for the various core components of cloud computing?

- A. SP 800-153
- B. SP 800-145
- C. SP 800-53
- D. SP 800-40

Answer: B

Explanation:

NIST Special Publications 800-145 is titled "The NIST Definition of Cloud Computing" and contains definitions and explanations of core cloud concepts and components.

NEW QUESTION 477

- (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 479

- (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 480

- (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 485

- (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 488

- (Exam Topic 1)

What is the biggest negative to leasing space in a data center versus building or maintain your own?

- A. Costs
- B. Control
- C. Certification
- D. Regulation

Answer: B

Explanation:

When leasing space in a data center, an organization will give up a large degree of control as to how it is built and maintained, and instead must conform to the policies and procedures of the owners and operators of the data center.

NEW QUESTION 491

- (Exam Topic 1)

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

- A. 30-50 percent relative humidity
- B. 50-75 percent relative humidity
- C. 20-40 percent relative humidity
- D. 40-60 percent relative humidity

Answer: D

Explanation:

The guidelines from ASHRAE establish 40-60 percent relative humidity as optimal for a data center.

NEW QUESTION 495

- (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 500

- (Exam Topic 1)

Which of the following threat types can occur when baselines are not appropriately applied or unauthorized changes are made?

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

Answer: C

Explanation:

Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner. This can be caused from a shortcoming in security baselines or configurations, unauthorized changes to system configurations, or a failure to patch and upgrade systems as the vendor releases security patches.

NEW QUESTION 501

- (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 502

- (Exam Topic 1)

What type of PII is regulated based on the type of application or per the conditions of the specific hosting agreement?

- A. Specific
- B. Contractual
- C. regulated
- D. Jurisdictional

Answer: B

Explanation:

Contractual PII has specific requirements for the handling of sensitive and personal information, as defined at a contractual level. These specific requirements will typically document the required handling procedures and policies to deal with PII. They may be in specific security controls and configurations, required policies or procedures, or limitations on who may gain authorized access to data and systems.

NEW QUESTION 505

- (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 509

- (Exam Topic 1)

Which of the following roles involves the connection and integration of existing systems and services to a cloud environment?

- A. Cloud service business manager
- B. Cloud service user
- C. Cloud service administrator
- D. Cloud service integrator

Answer: D

Explanation:

The cloud service integrator is the official role that involves connecting and integrating existing systems and services with a cloud environment. This may involve moving services into a cloud environment, or connecting to external cloud services and capabilities from traditional data center-hosted services.

NEW QUESTION 513

- (Exam Topic 1)

Which of the following roles is responsible for preparing systems for the cloud, administering and monitoring services, and managing inventory and assets?

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

Answer: C

Explanation:

The cloud service operations manager is responsible for preparing systems for the cloud, administering and monitoring services, providing audit data as requested or required, and managing inventory and assets.

NEW QUESTION 515

- (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 518

- (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 520

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CCSP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CCSP Product From:

<https://www.2passeasy.com/dumps/CCSP/>

Money Back Guarantee

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 FirstTry
- * CCSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year