

Exam Questions CCSP

Certified Cloud Security Professional

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



NEW QUESTION 1

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 2

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 3

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 4

- (Exam Topic 4)

Which of the following is the best example of a key component of regulated PII?

- A. Audit rights of subcontractors
- B. Items that should be implemented
- C. PCI DSS
- D. Mandatory breach reporting

Answer: D

Explanation:

Mandatory breach reporting is the best example of regulated PII components. The rest are generally considered components of contractual PII.

NEW QUESTION 5

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 6

- (Exam Topic 4)

With the rapid emergence of cloud computing, very few regulations were in place that pertained to it specifically, and organizations often had to resort to using a collection of regulations that were not specific to cloud in order to drive audits and policies.

Which standard from the ISO/IEC was designed specifically for cloud computing?

- A. ISO/IEC 27001
- B. ISO/IEC 19889
- C. ISO/IEC 27001:2015
- D. ISO/IEC 27018

Answer: D

Explanation:

ISO/IEC 27018 was implemented to address the protection of personal and sensitive information within a cloud environment. ISO/IEC 27001 and its later 27001:2015 revision are both general-purpose data security standards. ISO/IEC 19889 is an erroneous answer.

NEW QUESTION 7

- (Exam Topic 4)

Data labels could include all the following, except:

- A. Data value
- B. Data of scheduled destruction
- C. Date data was created
- D. Data owner

Answer: A

Explanation:

All the others might be included in data labels, but we don't usually include data value, since it is prone to change frequently, and because it might not be information we want to disclose to anyone who does not have need to know.

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)

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

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

Answer: C

Explanation:

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

NEW QUESTION 10

- (Exam Topic 4)

What are the U.S. State Department controls on technology exports known as?

- A. DRM
- B. ITAR
- C. EAR
- D. EAL

Answer: B

Explanation:

ITAR is a Department of State program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Digital rights management tools are used for protecting electronic processing of intellectual property.

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 15

- (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 18

- (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 20

- (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 24

- (Exam Topic 4)

Which data sanitation method is also commonly referred to as "zeroing"?

- A. Overwriting
- B. Nullification
- C. Blanking
- D. Deleting

Answer: A

Explanation:

The zeroing of data--or the writing of null values or arbitrary data to ensure deletion has been fully completed--is officially referred to as overwriting. Nullification,

deleting, and blanking are provided as distractor terms.

NEW QUESTION 29

- (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 32

- (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 33

- (Exam Topic 4)

Which data protection strategy would be useful for a situation where the ability to remove sensitive data from a set is needed, but a requirement to retain the ability to map back to the original values is also present?

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

Answer: B

Explanation:

Tokenization involves the replacement of sensitive data fields with key or token values, which can ultimately be mapped back to the original, sensitive data values. Masking refers to the overall approach to covering sensitive data, and 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. Encryption refers to the overall process of protecting data via key pairs and protecting confidentiality.

NEW QUESTION 35

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 37

- (Exam Topic 4)

Gap analysis is performed for what reason?

- A. To begin the benchmarking process
- B. To assure proper accounting practices are being used
- C. To provide assurances to cloud customers
- D. To ensure all controls are in place and working properly

Answer: A

Explanation:

The primary purpose of the gap analysis is to begin the benchmarking process against risk and security standards and frameworks.

NEW QUESTION 39

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 42

- (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 43

- (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 47

- (Exam Topic 4)

The different cloud service models have varying levels of responsibilities for functions and operations depending with the model's level of service.

In which of the following models would the responsibility for patching lie predominantly with the cloud customer?

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

Answer: D

Explanation:

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

NEW QUESTION 49

- (Exam Topic 4)

Limits for resource utilization can be set at different levels within a cloud environment to ensure that no particular entity can consume a level of resources that impacts other cloud customers.

Which of the following is NOT a unit covered by limits?

- A. Hypervisor
- B. Cloud customer
- C. Virtual machine

D. Service

Answer: A

Explanation:

The hypervisor level, as a backend cloud infrastructure component, is not a unit where limits may be applied to control resource utilization. Limits can be placed at the service, virtual machine, and cloud customer levels within a cloud environment.

NEW QUESTION 53

- (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 56

- (Exam Topic 4)

What is one of the reasons a baseline might be changed?

- A. Numerous change requests
- B. To reduce redundancy
- C. Natural disaster
- D. Power fluctuation

Answer: A

Explanation:

If the CMB is receiving numerous change requests to the point where the amount of requests would drop by modifying the baseline, then that is a good reason to change the baseline. None of the other reasons should involve the baseline at all.

NEW QUESTION 60

- (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 62

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 63

- (Exam Topic 4)

Which of the following is NOT a major regulatory framework?

- A. PCI DSS
- B. HIPAA

- C. SOX
- D. FIPS 140-2

Answer: D

Explanation:

FIPS 140-2 is a United States certification standard for cryptographic modules, and it provides guidance and requirements for their use based on the requirements of the data classification. However, these are not actual regulatory requirements. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS) are all major regulatory frameworks either by law or specific to an industry.

NEW QUESTION 67

- (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 72

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 73

- (Exam Topic 4)

During the course of an audit, which of the following would NOT be an input into the control requirements used as part of a gap analysis.

- A. Contractual requirements
- B. Regulations
- C. Vendor recommendations
- D. Corporate policy

Answer: C

Explanation:

Vendor recommendations would not be pertinent to the gap analysis after an audit. Although vendor recommendations will typically play a role in the development of corporate policies or contractual requirements, they are not required. Regulations, corporate policy, and contractual requirements all determine the expected or mandated controls in place on a system.

NEW QUESTION 74

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 77

- (Exam Topic 4)

Data labels could include all the following, except:

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

Answer: A

Explanation:

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

NEW QUESTION 79

- (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 81

- (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 86

- (Exam Topic 4)

The baseline should cover which of the following?

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

Answer: C

Explanation:

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

NEW QUESTION 87

- (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 91

- (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 93

- (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 94

- (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 95

- (Exam Topic 4)

What concept does the A represent within the DREAD model?

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

Answer: A

Explanation:

The concept of affected users measures the percentage of users who would be impacted by a successful exploit. Scoring ranges from 0, which would impact no users, to 10, which would impact all users. None of the other options provided is the correct term.

NEW QUESTION 97

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 102

- (Exam Topic 4)

Many activities within a cloud environment are performed via programmatic means, where complex and distributed operations are handled without the need to perform each step individually.

Which of the following concepts does this describe?

- A. Orchestration
- B. Provisioning
- C. Automation
- D. Allocation

Answer: A

Explanation:

Orchestration is the programmatic means of managing and coordinating activities within a cloud environment and allowing for a commensurate level of automation and self-service. Provisioning, allocation, and automation are all components of orchestration, but none refers to the overall concept.

NEW QUESTION 104

- (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 108

- (Exam Topic 4)

Proper implementation of DLP solutions for successful function requires which of the following?

- A. Physical access limitations
- B. USB connectivity
- C. Accurate data categorization
- D. Physical presence

Answer: C

Explanation:

DLP tools need to be aware of which information to monitor and which requires categorization (usually done upon data creation, by the data owners). DLPs can be implemented with or without physical access or presence. USB connectivity has nothing to do with DLP solutions.

NEW QUESTION 111

- (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 113

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 117

- (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 122

- (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 123

- (Exam Topic 4)

Identity and access management (IAM) is a security discipline that ensures which of the following?

- A. That all users are properly authorized
- B. That the right individual gets access to the right resources at the right time for the right reasons.
- C. That all users are properly authenticated
- D. That unauthorized users will get access to the right resources at the right time for the right reasons

Answer: B

Explanation:

Options A and C are also correct, but included in B, making B the best choice. D is incorrect, because we don't want unauthorized users gaining access.

NEW QUESTION 128

- (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 130

- (Exam Topic 4)

When using an IaaS solution, what is a key benefit provided to the customer?

- A. Metered and priced on the basis of units consumed

- B. Increased energy and cooling system efficiencies
- C. Transferred cost of ownership
- D. The ability to scale up infrastructure services based on projected usage

Answer: A

Explanation:

IaaS has a number of key benefits for organizations, which include but are not limited to these: -- Usage is metered and priced on the basis of units (or instances) consumed. This can also be billed back to specific departments or functions.

- It has an ability to scale up and down infrastructure services based on actual usage. This is particularly useful and beneficial where there are significant spikes and dips within the usage curve for infrastructure.
- It has a reduced cost of ownership. There is no need to buy assets for everyday use, no loss of asset value over time, and reduced costs of maintenance and support.
- It has a reduced energy and cooling costs along with "green IT" environment effect with optimum use of IT resources and systems.

NEW QUESTION 135

- (Exam Topic 4)

Best practices for key management include all of the following, except:

- A. Ensure multifactor authentication
- B. Pass keys out of band
- C. Have key recovery processes
- D. Maintain key security

Answer: A

Explanation:

We should do all of these except for requiring multifactor authentication, which is pointless in key management.

NEW QUESTION 138

- (Exam Topic 4)

DLP can be combined with what other security technology to enhance data controls?

- A. SIEM
- B. Hypervisors
- C. DRM
- D. Kerberos

Answer: C

Explanation:

DLP can be combined with DRM to protect intellectual property; both are designed to deal with data that falls into special categories. SIEMs are used for monitoring event logs, not live data movement. Kerberos is an authentication mechanism. Hypervisors are used for virtualization.

NEW QUESTION 139

- (Exam Topic 4)

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

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

Answer: C

Explanation:

Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discover potential vulnerabilities. Although the term malicious captures much of the intent of penetration testing from the perspective of an attacker, it is not the best answer. Static and dynamic are two types of system testing--where static is done offline and with knowledge of the system, and dynamic is done on a live system without any previous knowledge is associated--but neither describes the type of testing being asked for in the question.

NEW QUESTION 142

- (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 145

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 147

- (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 151

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 155

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 157

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 162

- (Exam Topic 4)

With a federated identity system, what does the identity provider send information to after a successful authentication?

- A. Relying party
- B. Service originator
- C. Service relay
- D. Service relay

Answer: A

Explanation:

Upon successful authentication, the identity provider sends an assertion with appropriate attributes to the relying party to grant access and assign appropriate roles to the user. The other terms provided are similar sounding to the correct term but are not actual components of a federated system.

NEW QUESTION 166

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 167

- (Exam Topic 4)

In the cloud motif, the data owner is usually:

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

Answer: C

Explanation:

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

NEW QUESTION 169

- (Exam Topic 4)

Which of the following is considered a technological control?

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

Answer: A

Explanation:

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

NEW QUESTION 170

- (Exam Topic 4)

There are many situations when testing a BCDR plan is appropriate or mandated. Which of the following would not be a necessary time to test a BCDR plan?

- A. After software updates
- B. After regulatory changes
- C. After major configuration changes
- D. Annually

Answer: B

Explanation:

Regulatory changes by themselves would not trigger a need for new testing of a BCDR plan. Any changes necessary for regulatory compliance would be accomplished through configuration changes or software updates, which in turn would then trigger the necessary new testing. Annual testing is crucial to any BCDR plan. Also, any time major configuration changes or software updates are done, the plan should be evaluated and tested to ensure it is still valid and complete.

NEW QUESTION 172

- (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 177

- (Exam Topic 4)

BCDR strategies do not typically involve the entire operations of an organization, but only those deemed critical to their business. Which concept pertains to the amount of services that need to be recovered to meet BCDR objectives?

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

Answer: A

Explanation:

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

NEW QUESTION 182

- (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 184

- (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 187

- (Exam Topic 4)

What must SOAP rely on for security since it does not provide security as a built-in capability?

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

Answer: A

Explanation:

Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for data passing, and it must rely on the encryption of those data packages for security. TLS and SSL (before it was deprecated) represent two common approaches to using encryption for protection of data transmissions. However, they are only two possible options and do not encapsulate the overall concept the question is looking for. Tokenization, which involves the replacement of sensitive data with opaque values, would not be appropriate for use with SOAP because the actual data is needed by the services.

NEW QUESTION 189

- (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 194

- (Exam Topic 4)

Which of the following is considered an administrative control?

- A. Keystroke logging
- B. Access control process
- C. Door locks
- D. Biometric authentication

Answer: B

Explanation:

A process is an administrative control; sometimes, the process includes elements of other types of controls (in this case, the access control mechanism might be a technical control, or it might be a physical control), but the process itself is administrative. Keystroke logging is a technical control (or an attack, if done for malicious purposes, and not for auditing); door locks are a physical control; and biometric authentication is a technological control.

NEW QUESTION 198

- (Exam Topic 4)

Your IT steering committee has, at a high level, approved your project to begin using cloud services. However, the committee is concerned with getting locked into a single cloud provider and has flagged the ability to easily move between cloud providers as a top priority. It also wants to save costs by reusing components. Which cross-cutting aspect of cloud computing would be your primary focus as your project plan continues to develop and you begin to evaluate cloud providers?

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

Answer: A

Explanation:

Interoperability is ability to easily move between cloud providers, by either moving or reusing components and services. This can pertain to any cloud deployment model, and it gives organizations the ability to constantly evaluate costs and services as well as move their business to another cloud provider as needed or desired. Portability relates to the wholesale moving of services from one cloud provider to another, not necessarily the reuse of components or services for other purposes. Although resiliency is not an official concept within cloud computing, it certainly would be found throughout other topics such as elasticity, auto-scaling, and resource pooling. Scalability pertains to changing resource allocations to a service to meet current demand, either upward or downward in scope.

NEW QUESTION 201

- (Exam Topic 4)

Being in a cloud environment, cloud customers lose a lot of insight and knowledge as to how their data is stored and their systems are deployed. Which concept from the ISO/IEC cloud standards relates to the necessity of the cloud provider to inform the cloud customer on these issues?

- A. Disclosure
- B. Transparency
- C. Openness
- D. Documentation

Answer: B

Explanation:

Transparency is the official process by which a cloud provider discloses insight and information into its configurations or operations to the appropriate audiences. Disclosure, openness, and documentation are all terms that sound similar to the correct answer, but none of them is the correct term in this case.

NEW QUESTION 205

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 208

- (Exam Topic 4)

A comprehensive BCDR plan will encapsulate many or most of the traditional concerns of operating a system in any data center. However, what is one consideration that is often overlooked with the formulation of a BCDR plan?

- A. Availability of staff
- B. Capacity at the BCDR site
- C. Restoration of services
- D. Change management processes

Answer: C

Explanation:

BCDR planning tends to focus so much on the failing over of services in the case of a disaster that recovery back to primary hosting after the disaster is often overlooked. In many instances, this can be just as complex a process as failing over, if not more so. Availability of staff, capacity at the BCDR site, and change management processes are typically integral to BCDR plans and are common components of them.

NEW QUESTION 211

- (Exam Topic 4)

Your company is in the planning stages of moving applications that have large data sets to a cloud environment.

What strategy for data removal would be the MOST appropriate for you to recommend if costs and speed are primary considerations?

- A. Shredding
- B. Media destruction
- C. Cryptographic erasure
- D. Overwriting

Answer: C

Explanation:

Cryptographic erasure involves having the data encrypted, typically as a matter of standard operations, and then rendering the data useless and unreadable by destroying the encryption keys for it. It represents a very cheap and immediate way to destroy data, and it works in all environments. With a cloud environment and multitenancy, media destruction or the physical destruction of storage devices, including shredding, would not be possible. Depending on the environment, overwriting may or may not be possible, but cryptographic erasure is the best answer because it is always an available option and is very quick to implement.

NEW QUESTION 214

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 219

- (Exam Topic 4)

Tokenization requires two distinct _____.

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

Answer: C

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 220

- (Exam Topic 3)

Where is a DLP solution generally installed when utilized for monitoring data in transit?

- A. Network perimeter
- B. Database server
- C. Application server
- D. Web server

Answer: A

Explanation:

To monitor data in transit, a DLP solution would optimally be installed at the network perimeter, to ensure that data leaving the network through various protocols conforms to security controls and policies. An application server or a web server would be more appropriate for monitoring data in use, and a database server would be an example of a location appropriate for monitoring data at rest.

NEW QUESTION 224

- (Exam Topic 3)

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

- A. Power feeds
- B. Chillers
- C. Network circuits
- D. Generators

Answer: B

Explanation:

Chillers and cooling systems are internal to a data center and its operations, and as such they are considered an internal redundancy. Power feeds, network circuits, and generators are all external to a data center and provide utility services to them, which makes them an external redundancy.

NEW QUESTION 225

- (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 230

- (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 233

- (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 236

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 237

- (Exam Topic 3)

Which cloud deployment model would be ideal for a group of universities looking to work together, where each university can gain benefits according to its specific needs?

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

Answer: D

Explanation:

A community cloud is owned and maintained by similar organizations working toward a common goal. In this case, the universities would all have very similar needs and calendar requirements, and they would not be financial competitors of each other. Therefore, this would be an ideal group for working together within a community cloud. A public cloud model would not work in this scenario because it is designed to serve the largest number of customers, would not likely be targeted toward specific requirements for individual customers, and would not be willing to make changes for them. A private cloud could accommodate such needs, but would not meet the criteria for a group working together, and a hybrid cloud spanning multiple cloud providers would not fit the specifics of the question.

NEW QUESTION 240

- (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 242

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 244

- (Exam Topic 3)

If a key feature of cloud computing that your organization desires is the ability to scale and expand without limit or concern about available resources, which cloud deployment model would you MOST likely be considering?

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

Answer: A

Explanation:

Public clouds, such as AWS and Azure, are massive systems run by major corporations, and they account for a significant share of Internet traffic and services. They are always expanding, offer enormous resources to customers, and are the least likely to run into resource constraints compared to the other deployment models. Private clouds would likely have the resources available for specific uses and could not be assumed to have a large pool of resources available for expansion. A community cloud would have the same issues as a private cloud, being targeted to similar organizations. A hybrid cloud, because it spans multiple clouds, would not fit the bill either, without the use of individual cloud models.

NEW QUESTION 248

- (Exam Topic 3)

With software-defined networking (SDN), which two types of network operations are segregated to allow for granularity and delegation of administrative access and functions?

- A. Filtering and forwarding
- B. Filtering and firewalling
- C. Firewalling and forwarding
- D. Forwarding and protocol

Answer: A

Explanation:

With SDN, the filtering and forwarding capabilities and administration are separated. This allows the cloud provider to build interfaces and management tools for administrative delegation of filtering configuration, without having to allow direct access to underlying network equipment. Firewalling and protocols are both terms related to networks, but they are not components SDN is concerned with.

NEW QUESTION 250

- (Exam Topic 3)

DNSSEC was designed to add a layer of security to the DNS protocol. Which type of attack was the DNSSEC extension designed to mitigate?

- A. Account hijacking
- B. Snooping
- C. Spoofing
- D. Data exposure

Answer: C

Explanation:

DNSSEC is an extension to the regular DNS protocol that utilizes digital signing of DNS query results, which can be verified to come from an authoritative source. This verification mitigates the ability for a rogue DNS server to be used to spoof query results and to direct users to malicious sites. DNSSEC provides for the verification of the integrity of DNS queries. It does not provide any protection from snooping or data exposure. Although it may help lessen account hijacking by preventing users from being directed to rogue sites, it cannot by itself eliminate the possibility.

NEW QUESTION 253

- (Exam Topic 3)

Which of the following threat types involves an application that does not validate authorization for portions of itself beyond when the user first enters it?

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

Answer: B

Explanation:

It is imperative that applications do checks when each function or portion of the application is accessed to ensure that the user is properly authorized. Without continual checks each time a function is accessed, an attacker could forge requests to access portions of the application where authorization has not been granted. 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. 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.

NEW QUESTION 254

- (Exam Topic 3)

Which of the following statements best describes a Type 1 hypervisor?

- A. The hypervisor software runs within an operating system tied to the hardware.
- B. The hypervisor software runs as a client on a server and needs an external service to administer it.
- C. The hypervisor software runs on top of an application layer.
- D. The hypervisor software runs directly on "bare metal" without an intermediary.

Answer: D

Explanation:

With a Type 1 hypervisor, the hypervisor software runs directly on top of the bare-metal system, without any intermediary layer or hosting system. None of these statements describes a Type 1 hypervisor.

NEW QUESTION 259

- (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 260

- (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 265

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 267

- (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 268

- (Exam Topic 3)

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 269

- (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 274

- (Exam Topic 3)

What type of storage structure does object storage employ to maintain files?

- A. Directory
- B. Hierarchical
- C. tree
- D. Flat

Answer: D

Explanation:

Object storage uses a flat file system to hold storage objects; it assigns files a key value that is then used to access them, rather than relying on directories or descriptive filenames. Typical storage layouts such as tree, directory, and hierarchical structures are used within volume storage, whereas object storage maintains a flat structure with key values.

NEW QUESTION 278

- (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 279

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 283

- (Exam Topic 3)

When dealing with PII, which category pertains to those requirements that can carry legal sanctions or penalties for failure to adequately safeguard the data and address compliance requirements?

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

Answer: C

Explanation:

Regulated PII pertains to data that is outlined in law and regulations. Violations of the requirements for the protection of regulated PII can carry legal sanctions or penalties. Contractual PII involves required data protection that is determined by the actual service contract between the cloud provider and cloud customer, rather than outlined by law. Violations of the provisions of contractual PII carry potential financial or contractual implications, but not legal sanctions. Legal and jurisdictional are similar terms to regulated, but neither is the official term used.

NEW QUESTION 285

- (Exam Topic 3)

Within a SaaS environment, what is the responsibility on the part of the cloud customer in regard to procuring the software used?

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

Answer: B

Explanation:

Within a SaaS implementation, the cloud customer licenses the use of the software from the cloud provider because SaaS delivers a fully functional application to the customer. With SaaS, the cloud provider is responsible for the entire software application and any necessary infrastructure to develop, run, and maintain it. The purchasing, development, and maintenance are fully the responsibility of the cloud provider.

NEW QUESTION 286

- (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 291

- (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 292

- (Exam Topic 3)

Humidity levels for a data center are a prime concern for maintaining electrical and computing resources properly as well as ensuring that conditions are optimal for top performance.

Which of the following is the optimal humidity level, as established by ASHRAE?

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

Answer: C

Explanation:

The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) recommends 40 to 60 percent relative humidity for data centers. None of these options is the recommendation from ASHRAE.

NEW QUESTION 294

- (Exam Topic 3)

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

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

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

Answer: D

Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry-regulatory standard, not a governmental one. The Sarbanes-Oxley Act (SOX) was passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders. The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

NEW QUESTION 295

- (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 296

- (Exam Topic 3)

Which of the following tasks within a SaaS environment would NOT be something the cloud customer would be responsible for?

- A. Authentication mechanism
- B. Branding
- C. Training

D. User access

Answer: A

Explanation:

The authentication mechanisms and implementations are the responsibility of the cloud provider because they are core components of the application platform and service. Within a SaaS implementation, the cloud customer will provision user access, deploy branding to the application interface (typically), and provide or procure training for its users.

NEW QUESTION 298

- (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 301

- (Exam Topic 3)

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

What does the management plane typically leverage for this orchestration?

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

Answer: A

Explanation:

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

NEW QUESTION 302

- (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 306

- (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 308

- (Exam Topic 3)

Which phase of the cloud data lifecycle would be the MOST appropriate for the use of DLP technologies to protect the data?

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

Answer: C

Explanation:

During the share phase, data is allowed to leave the application for consumption by other vendors, systems, or services. At this point, as the data is leaving the security controls of the application, the use of DLP technologies is appropriate to control how the data is used or to force expiration. During the use, create, and store phases, traditional security controls are available and are more appropriate because the data is still internal to the application.

NEW QUESTION 311

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 313

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 314

- (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 316

- (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 317

- (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 320

- (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 323

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the requirements placed on a system or application by law, policy, or requirements from standards?

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

Answer: A

Explanation:

Regulatory requirements are those imposed upon businesses and their operations either by law, regulation, policy, or standards and guidelines. These requirements are specific either to the locality in which the company or application is based or to the specific nature of the data and transactions conducted.

NEW QUESTION 325

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 328

- (Exam Topic 2)

Which of the cloud deployment models offers the easiest initial setup and access for the cloud customer?

- A. Hybrid

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

Answer: D

Explanation:

Because the public cloud model is available to everyone, in most instances all a customer will need to do to gain access is set up an account and provide a credit card number through the service's web portal. No additional contract negotiations, agreements, or specific group memberships are typically needed to get started.

NEW QUESTION 331

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 335

- (Exam Topic 2)

Which value refers to the amount of data an organization would need to recover in the event of a BCDR situation in order to reach an acceptable level of operations?

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

Answer: C

Explanation:

The recovery point objective (RPO) is defined as the amount of data a company would need to maintain and recover in order to function at a level acceptable to management. This may or may not be a restoration to full operating capacity, depending on what management deems as crucial and essential.

NEW QUESTION 337

- (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 341

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 344

- (Exam Topic 2)

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

- A. RSL
- B. RPO

- C. SRE
- D. RTO

Answer: D

Explanation:

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

NEW QUESTION 347

- (Exam Topic 2)

What is the biggest challenge to data discovery in a cloud environment?

- A. Format
- B. Ownership
- C. Location
- D. Multitenancy

Answer: C

Explanation:

With the distributed nature of cloud environments, the foremost challenge for data discovery is awareness of the location of data and keeping track of it during the constant motion of cloud storage systems.

NEW QUESTION 348

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 349

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Any application can be a possible target of denial-of-service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for non-authenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks.

NEW QUESTION 352

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 356

- (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 357

- (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 360

- (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 363

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 366

- (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 368

- (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 373

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 378

- (Exam Topic 2)

What type of security threat is DNSSEC designed to prevent?

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

Answer: C

Explanation:

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

NEW QUESTION 383

- (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 388

- (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 391

- (Exam Topic 2)

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

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

Answer: C

Explanation:

Tokenization is the practice of utilizing a random and opaque "token" value in data to replace what otherwise would be a sensitive or protected data object. The

token value is usually generated by the application with a means to map it back to the actual real value, and then the token value is placed in the data set with the same formatting and requirements of the actual real value so that the application can continue to function without different modifications or code changes.

NEW QUESTION 395

- (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 399

- (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 401

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 404

- (Exam Topic 2)

Who would be responsible for implementing IPsec to secure communications for an application?

- A. Developers
- B. Systems staff
- C. Auditors
- D. Cloud customer

Answer: B

Explanation:

Because IPsec is implemented at the system or network level, it is the responsibility of the systems staff. IPsec removes the responsibility from developers, whereas other technologies such as TLS would be implemented by developers.

NEW QUESTION 409

- (Exam Topic 2)

Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?

- A. Six months
- B. One month
- C. One year
- D. One week

Answer: A

Explanation:

SOC Type 2 reports are focused on the same policies and procedures, as well as their effectiveness, as SOC Type 1 reports, but are evaluated over a period of at least six consecutive months, rather than a finite point in time.

NEW QUESTION 412

- (Exam Topic 2)

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

- A. fencing
- B. Sandboxing
- C. Cellblocking
- D. Pooling

Answer: B

Explanation:

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

NEW QUESTION 417

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 418

- (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 419

- (Exam Topic 1)

Which of the following publishes the most commonly used standard for data center design in regard to tiers and topologies?

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

Answer: B

Explanation:

The Uptime Institute publishes the most commonly used and widely known standard on data center tiers and topologies. It is based on a series of four tiers, with each progressive increase in number representing more stringent, reliable, and redundant systems for security, connectivity, fault tolerance, redundancy, and cooling.

NEW QUESTION 420

- (Exam Topic 1)

What are the two protocols that TLS uses?

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

Answer: A

Explanation:

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

NEW QUESTION 423

- (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 426

- (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 427

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 431

- (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 432

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 433

- (Exam Topic 1)

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 435

- (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 436

- (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 439

- (Exam Topic 1)

What is the data encapsulation used with the SOAP protocol referred to?

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

Answer: B

Explanation:

Simple Object Access Protocol (SOAP) encapsulates its information in what is known as a SOAP envelope and then leverages common communications protocols for transmission.

NEW QUESTION 442

- (Exam Topic 1)

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

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

Answer: B

Explanation:

When leasing space in a data center, an organization can avoid the enormous startup and building costs associated with a data center, and can instead leverage economies of scale by grouping with other organizations and sharing costs.

NEW QUESTION 447

- (Exam Topic 1)

Which of the following cloud aspects complicates eDiscovery?

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

Answer: C

Explanation:

With multitenancy, eDiscovery becomes more complicated because the data collection involves extra steps to ensure that only those customers or systems that are within scope are turned over to the requesting authority.

NEW QUESTION 449

- (Exam Topic 1)

Which of the following standards primarily pertains to cabling designs and setups in a data center?

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

Answer: B

Explanation:

The standards put out by Building Industry Consulting Service International (BICSI) primarily cover complex cabling designs and setups for data centers, but also include specifications on power, energy efficiency, and hot/cold aisle setups.

NEW QUESTION 453

- (Exam Topic 1)

Why does a Type 1 hypervisor typically offer tighter security controls than a Type 2 hypervisor?

- A. A Type 1 hypervisor also controls patching of its hosted virtual machines ensure they are always secure.
- B. A Type 1 hypervisor is tied directly to the bare metal and only runs with code necessary to perform its specific mission.
- C. A Type 1 hypervisor performs hardware-level encryption for tighter security and efficiency.
- D. A Type 1 hypervisor only hosts virtual machines with the same operating systems as the hypervisor.

Answer: B

Explanation:

Type 1 hypervisors run directly on top of the bare metal and only contain the code and functions required to perform their purpose. They do not rely on any other systems or contain extra features to secure.

NEW QUESTION 458

- (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 463

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 466

- (Exam Topic 1)

Which of the following is not a component of contractual PII?

- A. Scope of processing
- B. Value of data
- C. Location of data
- D. Use of subcontractors

Answer: C

Explanation:

The value of data itself has nothing to do with it being considered a part of contractual

NEW QUESTION 469

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Due to the lack of an adequate privacy law or protection at the federal level in the United States, European privacy regulations generally prohibit the exporting or sharing of PII from Europe with the United States. Participation in the Safe Harbor program is voluntary on behalf of an organization, but it does require them to conform to specific requirements and policies that mirror those from the EU. Thus, organizations can fulfill requirements for data sharing and export and possibly serve customers in the EU.

NEW QUESTION 472

- (Exam Topic 1)

Which United States law is focused on accounting and financial practices of organizations?

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

Answer: C

Explanation:

The Sarbanes-Oxley (SOX) Act is not an act that pertains to privacy or IT security directly, but rather regulates accounting and financial practices used by organizations. It was passed to protect stakeholders and shareholders from improper practices and errors, and it sets forth rules for compliance, regulated and enforced by the Securities and Exchange Commission (SEC). The main influence on IT systems and operations is the requirements it sets for data retention, specifically in regard to what types of records must be preserved and for how long.

NEW QUESTION 474

- (Exam Topic 1)

Which of the following roles is responsible for overseeing customer relationships and the processing of financial transactions?

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

Answer: C

Explanation:

The cloud service business manager is responsible for overseeing business plans and customer relationships as well as processing financial transactions.

NEW QUESTION 478

.....

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