

ISC2

Exam Questions CCSP

Certified Cloud Security Professional



NEW QUESTION 1

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 2

- (Exam Topic 4)

Which of the following is considered a physical control?

- A. Fences
- B. Ceilings
- C. Carpets
- D. Doors

Answer: A

Explanation:

Fences are physical controls; carpets and ceilings are architectural features, and a door is not necessarily a control: the lock on the door would be a physical security control. Although you might think of a door as a potential answer, the best answer is the fence; the exam will have questions where more than one answer is correct, and the answer that will score you points is the one that is most correct.

NEW QUESTION 3

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 4

- (Exam Topic 4)

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 5

- (Exam Topic 4)

APIs are defined as which of the following?

- A. A set of protocols, and tools for building software applications to access a web-based software application or tool
- B. A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or tool
- C. A set of standards for building software applications to access a web-based software application or tool
- D. A set of routines and tools for building software applications to access web-based software applications

Answer: B

Explanation:

All the answers are true, but B is the most complete.

NEW QUESTION 6

- (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 7

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 8

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 9

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 10

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION 10

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 11

- (Exam Topic 4)

What type of masking would you employ to produce a separate data set for testing purposes based on production data without any sensitive information?

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

Answer: D

Explanation:

Static masking involves taking a data set and replacing sensitive fields and values with non-sensitive or garbage data. This is done to enable testing of an application against data that resembles production data, both in size and format, but without containing anything sensitive. Dynamic masking involves the live and transactional masking of data while an application is using it. Tokenized would refer to tokenization, which is the replacing of sensitive data with a key value that can later be matched back to the original value, and although it could be used as part of the production of test data, it does not refer to the overall process. Replicated is provided as an erroneous answer, as replicated data would be identical in value and would not accomplish the production of a test set.

NEW QUESTION 16

- (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 20

- (Exam Topic 4)

A data custodian is responsible for which of the following?

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

Answer: C

Explanation:

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

NEW QUESTION 24

- (Exam Topic 4)

Data labels could include all the following, except:

- A. Data value
- B. Date 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 27

- (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 32

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 34

- (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 35

- (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 37

- (Exam Topic 4)

As part of the auditing process, getting a report on the deviations between intended configurations and actual policy is often crucial for an organization.

What term pertains to the process of generating such a report?

- A. Deficiencies
- B. Findings
- C. Gap analysis
- D. Errors

Answer: C

Explanation:

The gap analysis determines if there are any differences between the actual configurations in use on systems and the policies that govern what the configurations are expected or mandated to be. The other terms provided are all similar to the correct answer ("findings" in particular is often used to articulate deviations in configurations), but gap analysis is the official term used.

NEW QUESTION 42

- (Exam Topic 4)

Which kind of SSAE audit report is most beneficial for a cloud customer, even though it's unlikely the cloud provider will share it?

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

Answer: C

Explanation:

The SOC 3 is the least detailed, so the provider is not concerned about revealing it. The SOC 1 Types 1 and 2 are about financial reporting and not relevant. The SOC 2 Type 2 is much more detailed and will most likely be kept closely held by the provider.

NEW QUESTION 47

- (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 49

- (Exam Topic 4)

Which of the following best describes a cloud carrier?

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

Answer: A

Explanation:

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

NEW QUESTION 51

- (Exam Topic 4)

Which of the following best describes the Organizational Normative Framework (ONF)?

- A. A set of application security, and best practices, catalogued and leveraged by the organization
- B. A container for components of an application's security, best practices catalogued and leveraged by the organization
- C. A framework of containers for some of the components of application security, best practices, catalogued and leveraged by the organization
- D. A framework of containers for all components of application security, best practices, catalogued and leveraged by the organization.

Answer: D

Explanation:

Option B is incorrect, because it refers to a specific applications security elements, meaning it is about an ANF, not the ONF. C is true, but not as complete as D, making D the better choice. C suggests that the framework contains only "some" of the components, which is why B (which describes "all" components) is better

NEW QUESTION 54

- (Exam Topic 4)

What is the Cloud Security Alliance Cloud Controls Matrix (CCM)?

- A. A set of software development life cycle requirements for cloud service providers
- B. An inventory of cloud services security controls that are arranged into a hierarchy of security domains
- C. An inventory of cloud service security controls that are arranged into separate security domains
- D. A set of regulatory requirements for cloud service providers

Answer: C

Explanation:

The CSA CCM is an inventory of cloud service security controls that are arranged into separate security domains, not a hierarchy.

NEW QUESTION 59

- (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 62

- (Exam Topic 4)

Which of the following best describes SAML?

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

Answer: D

NEW QUESTION 67

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 68

- (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 73

- (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 74

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 79

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 81

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 82

- (Exam Topic 4)

Which of the following is a management role, versus a technical role, as it pertains to data management and oversight?

- A. Data owner
- B. Data processor
- C. Database administrator
- D. Data custodian

Answer: A

Explanation:

Data owner is a management role that's responsible for all aspects of how data is used and protected. The database administrator, data custodian, and data processor are all technical roles that involve the actual use and consumption of data, or the implementation of security controls and policies with the data.

NEW QUESTION 86

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 91

- (Exam Topic 4)

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

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

Answer: C

Explanation:

EAR is a Commerce Department 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 95

- (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 96

- (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 98

- (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 103

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 108

- (Exam Topic 4)

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

- A. Data in transit

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

Answer: D

Explanation:

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

NEW QUESTION 111

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 114

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 118

- (Exam Topic 4)

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

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

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. Resource pooling and elasticity could both be impacted by insecure APIs, as both require automation and orchestration to operate properly, but automation is the better answer here. Redundancy would not be directly impacted by insecure APIs.

NEW QUESTION 121

- (Exam Topic 4)

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

Which of the following cloud concepts would this pertain to?

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

Answer: D

Explanation:

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

NEW QUESTION 123

- (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 126

- (Exam Topic 4)

In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?

- A. Physical
- B. All of the above
- C. technological
- D. Administrative

Answer: B

Explanation:

Layered defense calls for a diverse approach to security.

NEW QUESTION 128

- (Exam Topic 4)

What is a key capability or characteristic of PaaS?

- A. Support for a homogenous environment
- B. Support for a single programming language
- C. Ability to reduce lock-in
- D. Ability to manually scale

Answer: C

Explanation:

PaaS should have the following key capabilities and characteristics:

- Support multiple languages and frameworks: PaaS should support multiple programming languages and frameworks, thus enabling the developers to code in whichever language they prefer or the design requirements specify. In recent times, significant strides and efforts have been taken to ensure that open source stacks are both supported and utilized, thus reducing "lock-in" or issues with interoperability when changing CSPs.
- Multiple hosting environments: The ability to support a wide variety of underlying hosting environments for the platform is key to meeting customer requirements and demands. Whether public cloud, private cloud, local hypervisor, or bare metal, supporting multiple hosting environments allows the application developer or administrator to migrate the application when and as required. This can also be used as a form of contingency and continuity and to ensure the ongoing availability.
- Flexibility: Traditionally, platform providers provided features and requirements that they felt suited the client requirements, along with what suited their service offering and positioned them as the provider of choice, with limited options for the customers to move easily. This has changed drastically, with extensibility and flexibility now afforded to meeting the needs and requirements of developer audiences. This has been heavily influenced by open source, which allows relevant plug-ins to be quickly and efficiently introduced into the platform.
- Allow choice and reduce lock-in: PaaS learns from previous horror stories and restrictions, proprietary meant red tape, barriers, and restrictions on what developers could do when it came to migration or adding features and components to the platform. Although the requirement to code to specific APIs was made available by the providers, they could run their apps in various environments based on commonality and standard API structures, ensuring a level of consistency and quality for customers and users.
- Ability to auto-scale: This enables the application to seamlessly scale up and down as required to accommodate the cyclical demands of users. The platform will allocate resources and assign these to the application as required. This serves as a key driver for any seasonal organizations that experience spikes and drops in usage.

NEW QUESTION 132

- (Exam Topic 4)

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

- A. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the provider support
- B. The provider does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- C. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the provider support
- D. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- E. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the consumer support
- F. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- G. To deploy onto the cloud infrastructure provider-created or acquired applications created using programming languages, libraries, services, and tools that the provider support
- H. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Answer: B

Explanation:

According to "The NIST Definition of Cloud Computing," in PaaS, "the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

NEW QUESTION 133

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 137

- (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 138

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 142

- (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 146

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 149

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 150

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 155

- (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 159

- (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 162

- (Exam Topic 4)

Apart from using encryption at the file system level, what technology is the most widely used to protect data stored in an object storage system?

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

Answer: D

Explanation:

Information rights management (IRM) technologies allow security controls and policies to be enforced on a data object regardless of where it resides. They also allow for extended controls such as expirations and copying restrictions, which are not available through traditional control mechanisms. 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 and likely will be used in conjunction with other object data protection strategies.

NEW QUESTION 166

- (Exam Topic 4)

What are SOC 1/SOC 2/SOC 3?

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

Answer: A

Explanation:

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

NEW QUESTION 167

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 168

- (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 173

- (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 174

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 179

- (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 184

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 186

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 191

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 196

- (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 199

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 201

- (Exam Topic 4)

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 205

- (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 210

- (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 212

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 217

- (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 221

- (Exam Topic 4)

To protect data on user devices in a BYOD environment, the organization should consider requiring all the following, except:

- A. Multifactor authentication
- B. DLP agents
- C. Two-person integrity
- D. Local encryption

Answer: C

Explanation:

Although all the other options are ways to harden a mobile device, two-person integrity is a concept that has nothing to do with the topic, and, if implemented, would require everyone in your organization to walk around in pairs while using their mobile devices.

NEW QUESTION 222

- (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 227

- (Exam Topic 4)

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

- A. Scalability
- B. Interoperability

- C. Portability
- D. Reversibility

Answer: C

Explanation:

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

NEW QUESTION 232

- (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 237

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 241

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 242

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 244

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 247

- (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 252

- (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 254

- (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 258

- (Exam Topic 4)

Which of the following is not an example of a highly regulated environment?

- A. Financial services
- B. Healthcare
- C. Public companies
- D. Wholesale or distribution

Answer: D

Explanation:

Wholesalers or distributors are generally not regulated, although the products they sell may be.

NEW QUESTION 262

- (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 263

- (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 264

- (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 267

- (Exam Topic 4)

SOC Type 1 reports are considered "restricted use," in that they are intended only for limited audiences and purposes.

Which of the following is NOT a population that would be appropriate for a SOC Type 1 report?

- A. Current clients
- B. Auditors
- C. Potential clients
- D. The service organization

Answer: C

Explanation:

Potential clients are not served by SOC Type 1 audits. A Type 2 or Type 3 report would be appropriate for potential clients. SOC Type 1 reports are intended for restricted use, where only the service organization itself, current clients, or auditors would have access to them.

NEW QUESTION 271

- (Exam Topic 4)

Legal controls refer to which of the following?

- A. ISO 27001
- B. PCI DSS
- C. NIST 800-53r4
- D. Controls designed to comply with laws and regulations related to the cloud environment

Answer: D

Explanation:

Legal controls are those controls that are designed to comply with laws and regulations whether they be local or international.

NEW QUESTION 273

- (Exam Topic 4)

The BC/DR kit should include all of the following except:

- A. Annotated asset inventory
- B. Flashlight
- C. Hard drives
- D. Documentation equipment

Answer: C

Explanation:

While hard drives may be useful in the kit (for instance, if they store BC/DR data such as inventory lists, baselines, and patches), they are not necessarily required. All the other items should be included.

NEW QUESTION 274

- (Exam Topic 4)

Which of the following is a valid risk management metric?

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

Answer: B

Explanation:

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

NEW QUESTION 276

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 279

- (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 280

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 284

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 287

- (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 292

- (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 294

- (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 296

- (Exam Topic 4)

When beginning an audit, both the system owner and the auditors must agree on various aspects of the final audit report.

Which of the following would NOT be something that is predefined as part of the audit agreement?

- A. Size
- B. Format
- C. Structure
- D. Audience

Answer: A

Explanation:

The ultimate size of the audit report is not something that would ever be included in the audit scope or definition. Decisions about the content of the report should be the only factor that drives the ultimate size of the report. The structure, audience, and format of the audit report are all crucial elements that must be defined and agreed upon as part of the audit scope.

NEW QUESTION 298

- (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 299

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 301

- (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 303

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 306

- (Exam Topic 3)

What is a serious complication an organization faces from the compliance perspective with international operations?

- A. Multiple jurisdictions
- B. Different certifications
- C. Different operational procedures
- D. Different capabilities

Answer: A

Explanation:

When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, which often may not be clearly applicable or may be in contention with each other. These requirements can involve the location of the users and the type of data they enter into systems, the laws governing the organization that owns the application and any regulatory requirements they may have, and finally the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which may be multiple jurisdictions as well. Different certifications would not come into play as a challenge because the major IT and data center certifications are international and would apply to any cloud provider. Different capabilities and different operational procedures would be mitigated by the organization's selection of a cloud provider and would not be a challenge if an appropriate provider was chosen, regardless of location.

NEW QUESTION 309

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 313

- (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 318

- (Exam Topic 3)

The European Union is often considered the world leader in regard to the privacy of personal data and has declared privacy to be a "human right." In what year did the EU first assert this principle?

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

Answer: A

Explanation:

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

NEW QUESTION 319

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 321

- (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 322

- (Exam Topic 3)

If a cloud computing customer wishes to guarantee that a minimum level of resources will always be available, which of the following set of services would compromise the reservation?

- A. Memory and networking
- B. CPU and software
- C. CPU and storage
- D. CPU and memory

Answer: D

Explanation:

A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources.

A reservation pertains to memory and CPU resources. Under the concept of a reservation, memory and CPU are the guaranteed resources, but storage and networking are not included even though they are core components of cloud computing. Software would be out of scope for a guarantee and doesn't really pertain to the concept.

NEW QUESTION 324

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 325

- (Exam Topic 3)

With a cloud service category where the cloud customer is provided a full application framework into which to deploy their code and services, which storage types are MOST likely to be available to them?

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

Answer: A

Explanation:

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

NEW QUESTION 326

- (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 328

- (Exam Topic 3)

What does a cloud customer purchase or obtain from a cloud provider?

- A. Services
- B. Hosting
- C. Servers
- D. Customers

Answer: A

Explanation:

No matter what form they come in, "services" are obtained or purchased by a cloud customer from a cloud service provider. Services can come in many forms--virtual machines, network configurations, hosting setups, and software access, just to name a few. Hosting and servers--or, with a cloud, more appropriately virtual machines--are just two examples of "services" that a customer would purchase from a cloud provider. "Customers" would never be a service that's purchased.

NEW QUESTION 332

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 336

- (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 339

- (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 342

- (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 344

- (Exam Topic 3)

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 346

- (Exam Topic 3)

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

- A. Modify data
- B. Modify metadata
- C. New data
- D. Import data

Answer: B

Explanation:

Modifying the metadata does not change the actual data. Although this 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 is modified into a new form or value.

NEW QUESTION 347

- (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 350

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 354

- (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 358

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 359

- (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 363

- (Exam Topic 3)

Along with humidity, temperature is crucial to a data center for optimal operations and protection of equipment. Which of the following is the optimal temperature range as set by ASHRAE?

- A. 69.8 to 86.0 degrees Fahrenheit (21 to 30 degrees Celsius)
- B. 51.8 to 66.2 degrees Fahrenheit (11 to 19 degrees Celsius)
- C. 64.4 to 80.6 degrees Fahrenheit (18 to 27 degrees Celsius)
- D. 44.6 to 60.8 degrees Fahrenheit (7 to 16 degrees Celsius)

Answer: C

Explanation:

The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) recommends

NEW QUESTION 367

- (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 369

- (Exam Topic 3)

Firewalls are used to provide network security throughout an enterprise and to control what information can be accessed--and to a certain extent, through what means.

Which of the following is NOT something that firewalls are concerned with?

- A. IP address
- B. Encryption
- C. Port
- D. Protocol

Answer: B

Explanation:

Firewalls work at the network level and control traffic based on the source, destination, protocol, and ports. Whether or not the traffic is encrypted is not a factor with firewalls and their decisions about routing traffic. Firewalls work primarily with IP addresses, ports, and protocols.

NEW QUESTION 371

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 373

- (Exam Topic 3)

Where is a DLP solution generally installed when utilized for monitoring data at rest?

- A. Network firewall
- B. Host system
- C. Application server
- D. Database server

Answer: B

Explanation:

To monitor data at rest appropriately, the DLP solution would be installed on the host system where the data resides. A database server, in some situations, may be an appropriate answer, but the host system is the best answer because a database server is only one example of where data could reside. An application server processes data and typically sits between the data and presentation zones, and as such, does not store data at rest. A network firewall would be more appropriate for data in transit because it is not a place where data would reside.

NEW QUESTION 378

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 381

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 384

- (Exam Topic 3)

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

What type of attack is this?

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

Answer: A

Explanation:

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

NEW QUESTION 388

- (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 391

- (Exam Topic 3)

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 395

- (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 396

- (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 399

- (Exam Topic 3)

Digital investigations have adopted many of the same methodologies and protocols as other types of criminal or scientific inquiries.

What term pertains to the application of scientific norms and protocols to digital investigations?

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

Answer: D

Explanation:

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

NEW QUESTION 403

- (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 405

- (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 407

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 412

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 414

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 418

- (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 423

- (Exam Topic 3)

With a federated identity system, where would a user perform their authentication when requesting services or application access?

- A. Cloud provider
- B. The application
- C. Their home organization
- D. Third-party authentication system

Answer: C

Explanation:

With a federated identity system, a user will perform authentication with their home organization, and the application will accept the authentication tokens and user information from the identity provider in order to grant access. The purpose of a federated system is to allow users to authenticate from their home organization. Therefore, using the application or a third-party authentication system would be contrary to the purpose of a federated system because it necessitates the creation of additional accounts. The use of a cloud provider would not be relevant to the operations of a federated system.

NEW QUESTION 428

- (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 429

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 434

- (Exam Topic 3)

In order to ensure ongoing compliance with regulatory requirements, which phase of the cloud data lifecycle must be tested regularly?

- A. Archive
- B. Share
- C. Store
- D. Destroy

Answer: A

Explanation:

In order to ensure compliance with regulations, it is important for an organization to regularly test the restorability of archived data. As technologies change and older systems are deprecated, the risk rises for an organization to lose the ability to restore data from the format in which it is stored. With the destroy, store, and share phases, the currently used technologies will be sufficient for an organization's needs in an ongoing basis, so the risk that is elevated with archived data is not present.

NEW QUESTION 436

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 440

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 443

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 446

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 450

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the oversight of processes and systems, as well as to ensuring their compliance with specific policies and regulations?

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

Answer: D

Explanation:

Auditing involves reports and evidence that show user activity, compliance with controls and regulations, the systems and processes that run and what they do, as well as information and data access and modification records. A cloud environment adds additional complexity to traditional audits because the cloud customer will not have the same level of access to systems and data as they would in a traditional data center.

NEW QUESTION 452

- (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 455

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 456

- (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 458

- (Exam Topic 2)

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

- A. Scanning
- B. Probing
- C. Discovery
- D. Knowledge of the system

Answer: D

Explanation:

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

NEW QUESTION 459

- (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 464

- (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 468

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 473

- (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 478

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 479

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CCSP Practice Exam Features:

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

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