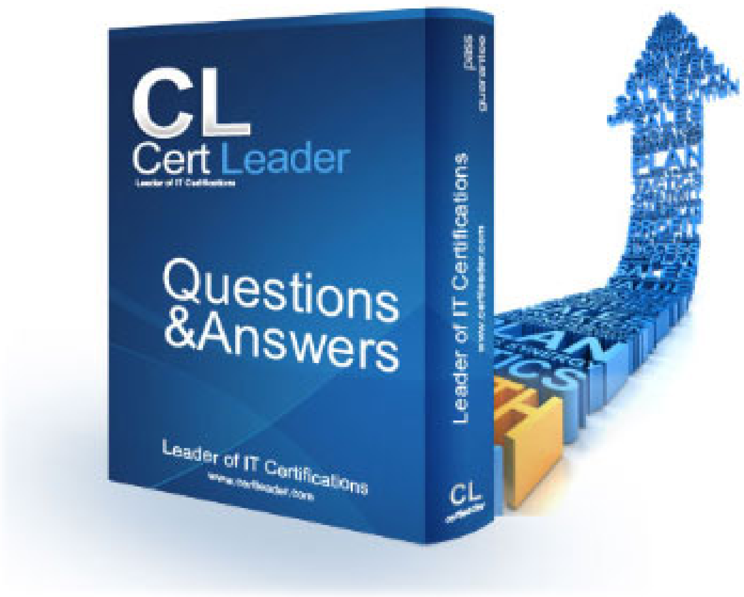
CCSP Dumps

Certified Cloud Security Professional

https://www.certleader.com/CCSP-dumps.html



NEW QUESTION 1
- (Exam Topic 4)
The cloud customer will have the most control of their data and systems, and the cloud provider will have the least amount of responsibility, in which cloud computing arrangement?

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

Answer: A

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

NEW QUESTION 2
- (Exam Topic 4)
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the required amount of time to restore services to the predetermined level?

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

Answer: C

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

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

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

Answer: D

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

NEW QUESTION 6
- (Exam Topic 4)
The most pragmatic option for data disposal in the cloud is which of the following?

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

Answer: A

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

NEW QUESTION 7
- (Exam Topic 4)
Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?

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

Answer: B

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

NEW QUESTION 8
- (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 9
- (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 10
- (Exam Topic 4)
Cryptographic keys for encrypted data stored in the cloud should be ________.

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

Answer: A

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

NEW QUESTION 10
- (Exam Topic 4)
Cloud systems are increasingly used for BCDR solutions for organizations. What aspect of cloud computing makes their use for BCDR the most attractive?

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

Answer: B

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

NEW QUESTION 14
- (Exam Topic 4)
DLP solutions can aid in deterring loss due to which of the following?

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

Answer: A

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

NEW QUESTION 16
- (Exam Topic 4)
What is the intellectual property protection for the tangible expression of a creative idea?

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

Answer: B

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

NEW QUESTION 17
- (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. One-time pads
B. Link encryption
C. Homomorphic encryption
D. AES

Answer: C

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

NEW QUESTION 20
- (Exam Topic 4)
What type of solution is at the core of virtually all directory services?

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

Answer: B

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

NEW QUESTION 21
- (Exam Topic 4)
What is an experimental technology that is intended to create the possibility of processing encrypted data without having to decrypt it first?

A. Quantum-state
B. Polyinstantiation
C. Homomorphic
D. Gastronomic

Answer: C

Explanation:
Homomorphic encryption hopes to achieve that goal; the other options are terms that have almost nothing to do with encryption.

NEW QUESTION 25
- (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 26
- (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 27
- (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 32
- (Exam Topic 4)
Which of the following best describes data masking?

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

Answer: A

Explanation:

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

NEW QUESTION 34
- (Exam Topic 4)
Which of the following technologies is NOT commonly used for accessing systems and services in a cloud environment in a secure manner?

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

Answer: A

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

NEW QUESTION 39
- (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 43
- (Exam Topic 4)
Deviations from the baseline should be investigated and _______.

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

Answer: B

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

NEW QUESTION 48
- (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 49
- (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 54
- (Exam Topic 4)
What does static application security testing (SAST) offer as a tool to the testers that makes it unique compared to other common security testing methodologies?

A. Live testing
B. Source code access
C. Production system scanning
D. Injection attempts

Answer: B

Explanation:
Static application security testing (SAST) is conducted against offline systems with previous knowledge of them, including their source code. Live testing is not part of static testing but rather is associated with dynamic testing. Production system scanning is not appropriate because static testing is done against offline systems. Injection attempts are done with many different types of testing and are not unique to one particular type. It is therefore not the best answer to the question.

NEW QUESTION 55
- (Exam Topic 4)
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:

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

Answer: C

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

NEW QUESTION 56
- (Exam Topic 4)
Data labels could include all the following, except:

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

Answer: B

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

NEW QUESTION 60
- (Exam Topic 4)
What is the correct order of the phases of the data life cycle?

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

Answer: D

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

NEW QUESTION 62
- (Exam Topic 4)
Different security testing methodologies offer different strategies and approaches to testing systems, requiring security personnel to determine the best type to use for their specific circumstances.
What does dynamic application security testing (DAST) NOT entail that SAST does?

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

Answer: B

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 it must be discovered during its testing. As with most types of testing, dynamic application security testing (DAST) involves probing, scanning, and a discovery process for system information.

NEW QUESTION 64
- (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 69
- (Exam Topic 4)
During the course of an audit, which of the following would NOT be an input into the control requirements used as part of a gap analysis.

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

Answer: C

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

NEW QUESTION 74
- (Exam Topic 4)
All policies within the organization should include a section that includes all of the following, except:

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

Answer: A

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

NEW QUESTION 75
- (Exam Topic 4)
Because of multitenancy, specific risks in the public cloud that don’t exist in the other cloud service models include all the following except:

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

Answer: A

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

NEW QUESTION 77
- (Exam Topic 4)
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 78

- (Exam Topic 4)
What masking strategy involves the replacing of sensitive data at the time it is accessed and used as it flows between the data and application layers of a service?

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

Answer: C

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

NEW QUESTION 81
- (Exam Topic 4)
With an application hosted in a cloud environment, who could be the recipient of an eDiscovery order?

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

Answer: B

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

NEW QUESTION 82
- (Exam Topic 4)
Because cloud providers will not give detailed information out about their infrastructures and practices to the general public, they will often use established auditing reports to ensure public trust, where the reputation of the auditors serves for assurance.
Which type of audit reports can be used for general public trust assurances?

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

Answer: C

Explanation:
SOC Type 3 audit reports are very similar to SOC Type 2, with the exception that they are intended for general release and public audiences.SAS-70 audits have been deprecated. SOC Type 1 audit reports have a narrow scope and are intended for very limited release, whereas SOC Type 2 audit reports are intended for wider audiences but not general release.

NEW QUESTION 85
- (Exam Topic 4)
Which of the following report is most aligned with financial control audits?

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

Answer: C

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

NEW QUESTION 88
- (Exam Topic 4)
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 91
- (Exam Topic 4)
A localized incident or disaster can be addressed in a cost-effective manner by using which of the following?

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

Answer: C

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

NEW QUESTION 93
- (Exam Topic 4)
Which of the following are cloud computing roles?

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

Answer: C

Explanation:
The following groups form the key roles and functions associated with cloud computing. They do not constitute an exhaustive list but highlight the main roles and functions within cloud computing:
- Cloud customer: An individual or entity that utilizes or subscribes to cloud based services or resources.
- CSP: A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations or individuals, usually for a fee; otherwise known to clients "as a service.
- Cloud backup service provider: A third-party entity that manages and holds operational responsibilities for cloud-based data backup services and solutions to customers from a central data center.
- CSB: Typically a third-party entity or company that looks to extend or enhance value to multiple customers of cloud-based services through relationships with multiple CSPs. It acts as a liaison between cloud services customers and CSPs, selecting the best provider for each customer and monitoring the services. The CSB can be utilized as a "middleman" to broker the best deal and customize services to the customer's requirements. May also resell cloud services.
- Cloud service auditor: Third-party organization that verifies attainment of SLAs.

NEW QUESTION 96
- (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 99
- (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 104
- (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 107
- (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 108
- (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 109
- (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 112
- (Exam Topic 4)
DLP can be combined with what other security technology to enhance data controls?

A. DRM
B. Hypervisor
C. SIEM
D. Kerberos

Answer: A

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 114
- (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 119
- (Exam Topic 4)
What are SOC 1/SOC 2/SOC 3?

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

Answer: A

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

NEW QUESTION 122
- (Exam Topic 4)
What are third-party providers of IAM functions for the cloud environment?

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

Answer: D

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

NEW QUESTION 125
- (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 128
- (Exam Topic 4)
Security is a critical yet often overlooked consideration for BCDR planning. At which stage of the planning process should security be involved?

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

Answer: A

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

NEW QUESTION 130
- (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 135
- (Exam Topic 4)
Identity and access management (IAM) is a security discipline that ensures which of the following?

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

Answer: B

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

NEW QUESTION 138
- (Exam Topic 4)
Which of the following terms is not associated with cloud forensics?

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

Answer: D

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

NEW QUESTION 139
- (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 142
- (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 discovery 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 143
- (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 145
- (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 150
- (Exam Topic 4)
Which of the following is NOT a commonly used communications method within cloud environments to secure data in transit?

A. IPSec
B. HTTPS
C. VPN
D. DNSSEC

Answer: D

Explanation:
DNSSEC is used as a security extension to DNS lookup queries in order to ensure the authenticity and authoritativeness of hostname resolutions, in order to prevent spoofing and redirection of traffic. Although it is a very important concept to be employed for security practices, it is not used to secure or encrypt data transmissions. HTTPS is the most commonly used security mechanism for data communications between clients and websites and web services. IPSec is less commonly used, but is also intended to secure communications between servers. VPN is commonly used to secure traffic into a network area or subnet for developers and administrative users.

NEW QUESTION 152
- (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 153
- (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 156
- (Exam Topic 4)
Which of the following components are part of what a CCSP should review when looking at contracting with a cloud service provider?

A. Redundant uplink grafts
B. Background checks for the provider's personnel
C. The physical layout of the datacenter
D. Use of subcontractors

Answer: D

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

NEW QUESTION 160
- (Exam Topic 4)
A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence.
Which core concept of cloud computing is most related to vendor lock-in?

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

Answer: C

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

NEW QUESTION 163
- (Exam Topic 4)
Which of the following is the dominant driver behind the regulations to which a system or application must adhere?

A. Data source
B. Locality
C. Contract
D. SLA

Answer: B

Explanation:
The locality--or physical location and jurisdiction where the system or data resides--is the dominant driver of regulations. This may be based on the type of data contained within the application or the way in which the data is used. The contract and SLA both articulate requirements for regulatory compliance and the responsibilities for the cloud provider and cloud customer, but neither artifact defines the actual requirements. Instead, the contract and SLA merely form the official documentation between the cloud provider and cloud customer. The source of the data may place contractual requirements or best practice guidelines on its usage, but ultimately jurisdiction has legal force and greater authority.

NEW QUESTION 168
- (Exam Topic 4)
What process entails taking sensitive data and removing the indirect identifiers from each data object so that the identification of a single entity would not be possible?

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

Answer: C

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

NEW QUESTION 169
- (Exam Topic 4)
Just like the risk management process, the BCDR planning process has a defined sequence of steps and processes to follow to ensure the production of a comprehensive and successful plan.
Which of the following is the correct sequence of steps for a BCDR plan?

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

Answer: A

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

NEW QUESTION 171
- (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 173
- (Exam Topic 4)
The various models generally available for cloud BC/DR activities include all of the following except:

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

Answer: D

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

NEW QUESTION 176
- (Exam Topic 4)
What category of PII data can carry potential fines or even criminal charges for its improper use or disclosure?

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

Answer: C

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

NEW QUESTION 180
- (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 184
- (Exam Topic 4)
When an organization is considering the use of cloud services for BCDR planning and solutions, which of the following cloud concepts would be the most important?

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

Answer: D

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

NEW QUESTION 186
- (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 189
- (Exam Topic 4)
Which of the following best describes the purpose and scope of ISO/IEC 27034-1?

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

Answer: D

NEW QUESTION 190
- (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 195
- (Exam Topic 4)
Which of the following is considered a technological control?

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

Answer: A

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

NEW QUESTION 198
- (Exam Topic 4)
In the cloud motif, the data processor is usually:

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

Answer: B

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

NEW QUESTION 201
- (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 203
- (Exam Topic 4)
Which of the following types of data would fall under data rights management (DRM) rather than information rights management (IRM)?

A. Personnel data
B. Security profiles
C. Publications
D. Financial records

Answer: C

Explanation:
Whereas IRM is used to protect a broad range of data, DRM is focused specifically on the protection of consumer media, such as publications, music, movies, and so on. IRM is used to protect general institution data, so financial records, personnel data, and security profiles would all fall under the auspices of IRM.

NEW QUESTION 208
- (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 213
- (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 217
- (Exam Topic 4)
Which of the following is not a risk management framework?

A. COBIT
B. Hex GBL
C. ISO 31000:2009
D. NIST SP 800-37

Answer: B

Explanation:
Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe. The rest are not.

NEW QUESTION 221
- (Exam Topic 4)
Your IT steering committee has, at a high level, approved your project to begin using cloud services. However, the committee is concerned with getting locked into a single cloud provider and has flagged the ability to easily move between cloud providers as a top priority. It also wants to save costs by reusing components. Which cross-cutting aspect of cloud computing would be your primary focus as your project plan continues to develop and you begin to evaluate cloud providers?

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

Answer: A

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

NEW QUESTION 224
- (Exam Topic 4)
Being in a cloud environment, cloud customers lose a lot of insight and knowledge as to how their data is stored and their systems are deployed.
Which concept from the ISO/IEC cloud standards relates to the necessity of the cloud provider to inform the cloud customer on these issues?

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

Answer: B

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

NEW QUESTION 225
- (Exam Topic 4)
Which is the lowest level of the CSA STAR program?

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

Answer: B

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

NEW QUESTION 230
- (Exam Topic 4)
Which of the following terms is NOT a commonly used category of risk acceptance?

A. Moderate
B. Critical
C. Minimal
D. Accepted

Answer: D

Explanation:

Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

NEW QUESTION 232
- (Exam Topic 4)
Whereas a contract articulates overall priorities and requirements for a business relationship, which artifact enumerates specific compliance requirements, metrics, and response times?

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

Answer: A

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

NEW QUESTION 236
- (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 infrastructur
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 interfac
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 infrastructur
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 interfac
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 infrastructur
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 interfac
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 infrastructur
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 interfac
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 240
- (Exam Topic 3)
The REST API is a widely used standard for communications of web-based services between clients and the servers hosting them.
Which protocol does the REST API depend on?

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

Answer: A

Explanation:
Representational State Transfer (REST) is a software architectural scheme that applies the components, connectors, and data conduits for many web applications used on the Internet. It uses and relies on the HTTP protocol and supports a variety of data formats. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data. Secure Shell client (SSH) is a secure method for allowing remote login to systems over a network.

NEW QUESTION 245
- (Exam Topic 3)
Where is a DLP solution generally installed when utilized for monitoring data in transit?

A. Network perimeter

B. Database server
C. Application server
D. Web server

Answer: A

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

NEW QUESTION 246
- (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:
SThe EU passed Directive 95/46 EC in 1995, which established data privacy as a human right. The other years listed are incorrect.

NEW QUESTION 250
- (Exam Topic 3)
With finite resources available within a cloud, even the largest cloud providers will at times need to determine which customers will receive additional resources first.
What is the term associated with this determination?

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

Answer: C

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

NEW QUESTION 252
- (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 254
- (Exam Topic 3)
A DLP solution/implementation has three main components. Which of the following is NOT one of the three main components?

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

Answer: C

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

NEW QUESTION 259
- (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 263
- (Exam Topic 3)
Where is an XML firewall most commonly and effectively deployed in the environment?

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

Answer: D

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

NEW QUESTION 266
- (Exam Topic 3)
During which phase of the cloud data lifecycle is it possible for the classification of data to change?

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

Answer: C

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

NEW QUESTION 269
- (Exam Topic 3)
Which cloud deployment model would be ideal for a group of universities looking to work together, where each university can gain benefits according to its specific needs?

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

Answer: D

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

NEW QUESTION 270
- (Exam Topic 3)
Which data state would be most likely to use digital signatures as a security protection mechanism?

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

Answer: A

Explanation:
During the data-in-use state, the information has already been accessed from storage and transmitted to the service, so reliance on a technology such as digital signatures is imperative to ensure security and complement the security methods used during previous states. Data in transit relies on technologies such as TLS to encrypt network transmission of packets for security. Data at rest primarily uses encryption for stored file objects. Archived data would be the same as data at rest.

NEW QUESTION 274
- (Exam Topic 3)
Your boss has tasked your team with getting your legacy systems and applications connected with new cloud-based services that management has decided are crucial to customer service and offerings.
Which role would you be assuming under this directive?

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

Answer: C

Explanation:
The cloud service integrator role is responsible for connecting and integrating existing services and applications with cloud-based services.A cloud service administrator is responsible for testing, monitoring, and securing cloud services, as well as providing usage reporting and dealing with service problems. The cloud service user is someone who consumes cloud services. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

NEW QUESTION 275
- (Exam Topic 3)
Within a federated identity system, which entity accepts tokens from the identity provider?

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

Answer: D

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

NEW QUESTION 276
- (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 280
- (Exam Topic 3)
Although much of the attention given to data security is focused on keeping data private and only accessible by authorized individuals, of equal importance is the trustworthiness of the data.
Which concept encapsulates this?

A. Validity
B. Integrity
C. Accessibility
D. Confidentiality

Answer: B

Explanation:
Integrity refers to the trustworthiness of data and whether its format and values are true and have not been corrupted or otherwise altered through unauthorized means. Confidentiality refers to keeping data from being access or viewed by unauthorized parties. Accessibility means that data is available and ready when needed by a user or service. Validity can mean a variety of things that are somewhat similar to integrity, but it's not the most appropriate answer in this case.

NEW QUESTION 283
- (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 287
- (Exam Topic 3)
Which cloud storage type requires special consideration on the part of the cloud customer to ensure they do not program themselves into a vendor lock-in situation?

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

Answer: D

Explanation:
Structured storage is designed, maintained, and implemented by a cloud service provider as part of a PaaS offering. It is specific to that cloud provider and the way they have opted to implement systems, so special care is required to ensure that applications are not designed in a way that will lock the cloud customer into a specific cloud provider with that dependency. Unstructured storage for auxiliary files would not lock a customer into a specific provider. With volume and object storage, because the cloud customer maintains their own systems with IaaS, moving and replicating to a different cloud provider would be very easy.

NEW QUESTION 292
- (Exam Topic 3)
Many of the traditional concepts of systems and services for a traditional data center also apply to the cloud. Both are built around key computing concepts. Which of the following compromise the two facets of computing?

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

Answer: C

Explanation:
The CPU and memory resources of an environment together comprise its "computing" resources. Cloud environments, especially public clouds, are enormous pools of resources for computing and are typically divided among a large number of customers with constantly changing needs and demands. Although storage and networking are core components of a cloud environment, they do not comprise its computing core. Software, much like within a traditional data center, is highly subjective based on the application, system, service, or cloud computing model used; however, it is not one of the core cloud components.

NEW QUESTION 296
- (Exam Topic 3)
Which of the following statements best describes a Type 1 hypervisor?

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

Answer: D

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

NEW QUESTION 298
- (Exam Topic 3)
Which data state would be most likely to use TLS as a protection mechanism?

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

Answer: D

Explanation:
TLS would be used with data in transit, when packets are exchanged between clients or services and sent across a network. During the data-in-use state, the data

is already protected via a technology such as TLS as it is exchanged over the network and then relies on other technologies such as digital signatures for protection while being used. The data-at-rest state primarily uses encryption for stored file objects. Archived data would be the same as data at rest.

NEW QUESTION 300
4 to 80.6 degrees Fahrenheit (or 18 to 27 degrees Celsius) as the optimal temperature range for data centers. None of these options is the recommendation from ASHRAE.

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 305
- (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 306
- (Exam Topic 3)
There is a large gap between the privacy laws of the United States and those of the European Union. Bridging this gap is necessary for American companies to do business with European companies and in European markets in many situations, as the American companies are required to comply with the stricter requirements. Which US program was designed to help companies overcome these differences?

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

Answer: D

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

NEW QUESTION 308
- (Exam Topic 3)
Which of the following threat types involves the sending of commands or arbitrary data through input fields in an application in an attempt to get that code executed as part of normal processing?

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

Answer: C

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

NEW QUESTION 312
- (Exam Topic 3)
Which of the following threat types involves leveraging a user's browser to send untrusted data to be executed with legitimate access via the user’s valid credentials?

A. Injection
B. Missing function-level access control

C. Cross-site scripting
D. Cross-site request forgery

Answer: D

Explanation:
Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or perhaps the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with their own access and permissions, allowing the attacker to redirect the user's web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access. 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 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 313
- (Exam Topic 3)
The share phase of the cloud data lifecycle involves allowing data to leave the application, to be shared with external systems, services, or even other vendors/contractors.
What technology would be useful for protecting data at this point?

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

Answer: B

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

NEW QUESTION 317
- (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 320
- (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 322
- (Exam Topic 3)
Where is a DLP solution generally installed when utilized for monitoring data in use?

A. Application server
B. Database server
C. Network perimeter
D. User's client

Answer: D

Explanation:
To monitor data in use, the DLP solution's optimal location would be on the user's client or workstation, where the data would be used or processed, and where it would be most vulnerable to access or exposure. The network perimeter is most appropriate for data in transit, and an application server would serve as middle stage between data at rest and data in use, but is a less correct answer than a user's client. A database server would be an example of a location appropriate for monitoring data at rest.

NEW QUESTION 326
- (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 331
- (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 335
- (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 340
- (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 342
- (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 343
- (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 347
- (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 relatively humidity for data centers. None of these options is the recommendation from ASHRAE.

NEW QUESTION 349
- (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 350
- (Exam Topic 3)
Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.
Which of the following is NOT a regulatory system from the United States federal government?

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

Answer: D

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

NEW QUESTION 351
- (Exam Topic 3)
A crucial decision any company must make is in regard to where it hosts the data systems it depends on. A debate exists as to whether it's best to lease space in a data center or build your own data center--and now with cloud computing, whether to purchase resources within a cloud.
What is the biggest advantage to leasing space in a data center versus procuring cloud services?

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

Answer: B

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

NEW QUESTION 354
- (Exam Topic 3)
Which of the following is NOT one of the main intended goals of a DLP solution?

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

Answer: B

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

NEW QUESTION 359
- (Exam Topic 3)
Which of the following tasks within a SaaS environment would NOT be something the cloud customer would be responsible for?

A. Authentication mechanism
B. Branding
C. Training
D. User access

Answer: A

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

NEW QUESTION 360
- (Exam Topic 3)
Many tools and technologies are available for securing or monitoring data in transit within a data center, whether it is a traditional data center or a cloud.
Which of the following is NOT a technology for securing data in transit?

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

Answer: C

Explanation:

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

NEW QUESTION 363
- (Exam Topic 3)
The management plane is used to administer a cloud environment and perform administrative tasks across a variety of systems, but most specifically it's used with the hypervisors.
What does the management plane typically leverage for this orchestration?

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

Answer: A

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

NEW QUESTION 368
- (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 369
- (Exam Topic 3)
Many aspects and features of cloud computing can make eDiscovery compliance more difficult or costly. Which aspect of cloud computing would be the MOST complicating factor?

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

Answer: C

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

NEW QUESTION 372
- (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 374
- (Exam Topic 3)
From the perspective of compliance, what is the most important consideration when it comes to data center location?

A. Natural disasters
B. Utility access
C. Jurisdiction
D. Personnel access

Answer: C

Explanation:
Jurisdiction will dictate much of the compliance and audit requirements for a data center. Although all the aspects listed are very important to security, from a strict compliance perspective, jurisdiction is the most important. Personnel access, natural disasters, and utility access are all important operational considerations for selecting a data center location, but they are not related to compliance issues like jurisdiction is.

NEW QUESTION 378
- (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 383
- (Exam Topic 2)
Which of the following is a widely used tool for code development, branching, and collaboration?

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

Answer: A

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

NEW QUESTION 384
- (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 385
- (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 387
- (Exam Topic 2)
Which of the following is NOT a function performed by the handshake protocol of TLS?

A. Key exchange
B. Encryption
C. Negotiation of connection
D. Establish session ID

Answer: B

Explanation:
The handshake protocol negotiates and establishes the connection as well as handles the key exchange and establishes the session ID. It does not perform the actual encryption of data packets.

NEW QUESTION 390
- (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 393
- (Exam Topic 2)
Which of the following is NOT a key area for performance monitoring as far as an SLA is concerned?

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

Answer: B

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

NEW QUESTION 394
- (Exam Topic 2)
Which of the following is the sole responsibility of the cloud provider, regardless of which cloud model is used?

A. Platform
B. Data
C. Physical environment
D. Infrastructure

Answer: C

Explanation:
Regardless of which cloud-hosting model is used, the cloud provider always has sole responsibility for the physical environment.

NEW QUESTION 397
- (Exam Topic 2)
Which of the following does NOT fall under the "IT" aspect of quality of service (QoS)?

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

Answer: B

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

NEW QUESTION 399
- (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 404
- (Exam Topic 2)
Which process serves to prove the identity and credentials of a user requesting access to an application or data?

A. Repudiation
B. Authentication
C. Identification
D. Authorization

Answer: B

Explanation:
Authentication is the process of proving whether the identity presented by a user is true and valid. This can be done through common mechanisms such as user ID and password combinations or with more secure methods such as multifactor authentication.

NEW QUESTION 406
- (Exam Topic 2)
Which value refers to the amount of data an organization would need to recover in the event of a BCDR situation in order to reach an acceptable level of operations?

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

Answer: C

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

NEW QUESTION 410
- (Exam Topic 2)
Which aspect of security is DNSSEC designed to ensure?

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

Answer: A

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

NEW QUESTION 411
- (Exam Topic 2)
What process is used within a cloud environment to maintain resource balancing and ensure that resources are available where and when needed?

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

Answer: D

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

NEW QUESTION 416
- (Exam Topic 2)
What is the biggest challenge to data discovery in a cloud environment?

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

Answer: C

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

NEW QUESTION 418
- (Exam Topic 2)
What concept does the "D" represent with the STRIDE threat model?

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

Answer: B

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

NEW QUESTION 423
- (Exam Topic 2)
Which of the following is a commonly used tool for maintaining system configurations?

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

Answer: C

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

NEW QUESTION 428
- (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 433
- (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 438
- (Exam Topic 2)
From a security perspective, which of the following is a major concern when evaluating possible BCDR solutions?

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

Answer: C

Explanation:
When a security professional is considering cloud solutions for BCDR, a top concern is the jurisdiction where the cloud systems are hosted. If the jurisdiction is

different from where the production systems are hosted, they may be subjected to different regulations and controls, which would make a seamless BCDR solution far more difficult.

NEW QUESTION 440
- (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 444
- (Exam Topic 2)
With software-defined networking, what aspect of networking is abstracted from the forwarding of traffic?

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

Answer: C

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

NEW QUESTION 449
- (Exam Topic 2)
Which of the following is NOT an application or utility to apply and enforce baselines on a system?

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

Answer: B

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

NEW QUESTION 450
- (Exam Topic 2)
Which of the following service categories entails the least amount of support needed on the part of the cloud customer?

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

Answer: A

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

NEW QUESTION 454
- (Exam Topic 2)
Which of the following is NOT a factor that is part of a firewall configuration?

A. Encryption
B. Port
C. Protocol
D. Source IP

Answer: A

Explanation:
Firewalls take into account source IP, destination IP, the port the traffic is using, as well as the network protocol (UDP/TCP). Whether or not the traffic is encrypted

is not something a firewall is concerned with.

NEW QUESTION 455
- (Exam Topic 2)
What concept does the "A" represent in the DREAD model?

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

Answer: A

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

NEW QUESTION 457
- (Exam Topic 2)
Which type of controls are the SOC Type 1 reports specifically focused on?

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

Answer: C

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

NEW QUESTION 462
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the assigning of jobs, tasks, and roles, as well as to ensuring they are successful and properly performed?

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

Answer: B

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

NEW QUESTION 467
- (Exam Topic 2)
What is a standard configuration and policy set that is applied to systems and virtual machines called?

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

Answer: B

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

NEW QUESTION 469
- (Exam Topic 2)
What is an often overlooked concept that is essential to protecting the confidentiality of data?

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

Answer: B

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

NEW QUESTION 474
- (Exam Topic 2)
Which European Union directive pertains to personal data privacy and an individual's control over their personal data?

A. 99/9/EC
B. 95/46/EC
C. 2000/1/EC
D. 2013/27001/EC

Answer: B

Explanation:
Directive 95/46/EC is titled "On the protection of individuals with regard to the processing of personal data and on the free movement of such data."

NEW QUESTION 479
- (Exam Topic 2)
What provides the information to an application to make decisions about the authorization level appropriate when granting access?

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

Answer: D

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

NEW QUESTION 484
- (Exam Topic 2)
What type of masking strategy involves replacing data on a system while it passes between the data and application layers?

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

Answer: A

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

NEW QUESTION 489
- (Exam Topic 2)
Which security concept is based on preventing unauthorized access to data while also ensuring that it is accessible to those authorized to use it?

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

Answer: C

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

NEW QUESTION 494
......