ISC2

Exam Questions CCSP

Certified Cloud Security Professional

NEW QUESTION 1
- (Exam Topic 4)
All of the following are techniques to enhance the portability of cloud data, in order to minimize the potential of vendor lock-in except:

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

Answer: B

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

NEW QUESTION 2
- (Exam Topic 4)
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 storage types is most closely associated with a database-type storage implementation?

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

Answer: D

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

NEW QUESTION 4
- (Exam Topic 4)
In which cloud service model is the customer required to maintain the OS?

A. Iaas
B. CaaS
C. PaaS
D. SaaS

Answer: A

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

NEW QUESTION 5
- (Exam Topic 4)
Which ITIL component is an ongoing, iterative process of tracking all deployed and configured resources that an organization uses and depends on, whether they are hosted in a traditional data center or a cloud?

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

Answer: D

Explanation:
Configuration management tracks and maintains detailed information about all IT components within an organization. Availability management is focused on

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

NEW QUESTION 6
- (Exam Topic 4)
Which of the following concepts is NOT one of the core components to an encryption system architecture?

A. Software
B. Network
C. Keys
D. Data

Answer: B

Explanation:
The network utilized is not one of the key components of an encryption system architecture. In fact, a network is not even required for encryption systems or the processing and protection of data. The data, software used for the encryption engine itself, and the keys used to implement the encryption are all core components of an encryption system architecture.

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

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

Answer: C

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

NEW QUESTION 9
- (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 10
- (Exam Topic 4)
Which of the following best describes a cloud carrier?

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

Answer: A

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

NEW QUESTION 10
- (Exam Topic 4)
What is the Cloud Security Alliance Cloud Controls Matrix (CCM)?

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

Answer: C

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

NEW QUESTION 15
- (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 16
- (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 17
- (Exam Topic 4)
Which of the following frameworks focuses specifically on design implementation and management?

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

Answer: A

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

NEW QUESTION 21
- (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 22
- (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 25
- (Exam Topic 4)
Gap analysis is performed for what reason?

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

Answer: A

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

NEW QUESTION 28
- (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 32
- (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 33
- (Exam Topic 4)
Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider?

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

Answer: C

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

NEW QUESTION 36
- (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 37
- (Exam Topic 4)
Data labels could include all the following, except:

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

Answer: A

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

NEW QUESTION 42
- (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 44
- (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 49
- (Exam Topic 4)
Which format is the most commonly used standard for exchanging information within a federated identity system?

A. XML
B. HTML
C. SAML
D. JSON

Answer: C

Explanation:
Security Assertion Markup Language (SAML) is the most common data format for information exchange within a federated identity system. It is used to transmit and exchange authentication and authorization data.XML is similar to SAML, but it's used for general-purpose data encoding and labeling and is not used for the exchange of authentication and authorization data in the way that SAML is for federated systems. JSON is used similarly to XML, as a text-based data exchange format that typically uses attribute-value pairings, but it's not used for authentication and authorization exchange. HTML is used only for encoding web pages for web browsers and is not used for data exchange--and certainly not in a federated system.

NEW QUESTION 53
- (Exam Topic 4)
Which of the following is NOT considered a type of data loss?

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

Answer: B

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

NEW QUESTION 55
- (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 57
- (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 61
- (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 65
- (Exam Topic 4)
Key maintenance and security are paramount within a cloud environment due to the widespread use of encryption for both data and transmissions.
Which of the following key-management systems would provide the most robust control over and ownership of the key-management processes for the cloud customer?

A. Remote key management service
B. Local key management service
C. Client key management service
D. Internal key management service

Answer: A

Explanation:
A remote key management system resides away from the cloud environment and is owned and controlled by the cloud customer. With the use of a remote service, the cloud customer can avoid being locked into a proprietary system from the cloud provider, but also must ensure that service is compatible with the services offered by the cloud provider. A local key management system resides on the actual servers using the keys, which does not provide optimal security or control over

them. Both the terms internal key management service and client key management service are provided as distractors.

NEW QUESTION 66
- (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 71
- (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 74
- (Exam Topic 4)
Data masking can be used to provide all of the following functionality, except:

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

Answer: C

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

NEW QUESTION 77
- (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 81
- (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 86
- (Exam Topic 4)
In a cloud environment, encryption should be used for all the following, except:

A. Secure sessions/VPN
B. Long-term storage of data
C. Near-term storage of virtualized images
D. Profile formatting

Answer: D

Explanation:
All of these activities should incorporate encryption, except for profile formatting, which is a made-up term.

NEW QUESTION 88
- (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 91
- (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 95
- (Exam Topic 4)
Which of the following would be considered an example of insufficient due diligence leading to security or operational problems when moving to a cloud?

A. Monitoring
B. Use of a remote key management system
C. Programming languages used
D. Reliance on physical network controls

Answer: D

Explanation:
Many organizations in a traditional data center make heavy use of physical network controls for security. Although this is a perfectly acceptable best practice in a traditional data center, this reliance is not something that will port to a cloud environment. The failure of an organization to properly understand and adapt to the difference in network controls when moving to a cloud will likely leave an application with security holes and vulnerabilities. The use of a remote key management system, monitoring, or certain programming languages would not constitute insufficient due diligence by itself.

NEW QUESTION 96
- (Exam Topic 4)
For optimal security, trust zones are used for network segmentation and isolation. They allow for the separation of various systems and tiers, each with its own security level.
Which of the following is typically used to allow administrative personnel access to trust zones?

A. IPSec
B. SSH

C. VPN
D. TLS

Answer: C

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

NEW QUESTION 100
- (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 102
- (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 103
- (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 105
- (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 106
- (Exam Topic 4)
With a federated identity system, what does the identity provider send information to after a successful authentication?

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

Answer: A

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

NEW QUESTION 111
- (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 114
- (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 116
- (Exam Topic 4)
There are many situations when testing a BCDR plan is appropriate or mandated. Which of the following would not be a necessary time to test a BCDR plan?

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

Answer: B

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

NEW QUESTION 118
- (Exam Topic 4)
To address shared monitoring and testing responsibilities in a cloud configuration, the provider might offer all these to the cloud customer except:

A. Access to audit logs and performance data
B. DLP solution results
C. Security control administration
D. SIM, SEI
E. and SEM logs

Answer: C

Explanation:
While the provider might share any of the other options listed, the provider will not share administration of security controls with the customer. Security controls are the sole province of the provider.

NEW QUESTION 122
- (Exam Topic 4)
What is the cloud service model in which the customer is responsible for administration of the OS?

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

Answer: D

Explanation:
In IaaS, the cloud provider only owns the hardware and supplies the utilities. The customer is responsible for the OS, programs, and data. In PaaS and SaaS, the provider also owns the OS. There is no QaaS. That is a red herring.

NEW QUESTION 123
- (Exam Topic 4)
Which of the following is a valid risk management metric?

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

Answer: B

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

NEW QUESTION 128
- (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 130
- (Exam Topic 4)
Which of the following is considered an administrative control?

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

Answer: B

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

NEW QUESTION 134
- (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 139
- (Exam Topic 4)
In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?

A. HIPAA
B. The contract
C. Statutes
D. Security control matrix

Answer: B

Explanation:
The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable. The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

NEW QUESTION 143
- (Exam Topic 4)
A comprehensive BCDR plan will encapsulate many or most of the traditional concerns of operating a system in any data center.
However, what is one consideration that is often overlooked with the formulation of a BCDR plan?

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

Answer: C

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

NEW QUESTION 144
- (Exam Topic 4)
When beginning an audit, both the system owner and the auditors must agree on various aspects of the final audit report.
Which of the following would NOT be something that is predefined as part of the audit agreement?

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

Answer: A

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

NEW QUESTION 145
- (Exam Topic 4)
Tokenization requires two distinct ________.

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

Answer: C

Explanation:
In order to implement tokenization, there will need to be two databases: the database containing the raw, original data, and the token database containing tokens that map to original data. Having two-factor authentication is nice, but certainly not required. Encryption keys are not necessary for tokenization. Two-person integrity does not have anything to do with tokenization.

NEW QUESTION 147
- (Exam Topic 3)
Which of the following aspects of security is solely the responsibility of the cloud provider?

A. Regulatory compliance
B. Physical security

C. Operating system auditing
D. Personal security of developers

Answer: B

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

NEW QUESTION 148
- (Exam Topic 3)
Modern web service systems are designed for high availability and resiliency. Which concept pertains to the ability to detect problems within a system, environment, or application and programmatically invoke redundant systems or processes for mitigation?

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

Answer: C

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

NEW QUESTION 151
- (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 153
- (Exam Topic 3)
Jurisdictions have a broad range of privacy requirements pertaining to the handling of personal data and information.
Which jurisdiction requires all storage and processing of data that pertains to its citizens to be done on hardware that is physically located within its borders?

A. Japan
B. United States
C. European Union
D. Russia

Answer: D

Explanation:
The Russian government requires all data and processing of information about its citizens to be done solely on systems and applications that reside within the physical borders of the country. The United States, European Union, and Japan focus their data privacy laws on requirements and methods for the protection of data, rather than where the data physically resides.

NEW QUESTION 155
- (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 158
- (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 163
- (Exam Topic 3)
If a key feature of cloud computing that your organization desires is the ability to scale and expand without limit or concern about available resources, which cloud deployment model would you MOST likely be considering?

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

Answer: A

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

NEW QUESTION 165
- (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 167
- (Exam Topic 3)
Which of the following roles would be responsible for managing memberships in federations and the use and integration of federated services?

A. Inter-cloud provider
B. Cloud service business manager
C. Cloud service administrator
D. Cloud service integrator

Answer: A

Explanation:
The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated services. A cloud service administrator is responsible for testing, monitoring, and securing cloud services, as well as providing usage reporting and dealing with service problems. The cloud service integrator is responsible for connecting existing systems and services with a cloud. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

NEW QUESTION 170
- (Exam Topic 3)
In the wake of many scandals with major corporations involving fraud and the deception of investors and regulators, which of the following laws was passed to govern accounting and financial records and disclosures?

A. GLBA

B. Safe Harbor
C. HIPAA
D. SOX

Answer: D

Explanation:
The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and accounting errors.The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy. The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Safe Harbor program was designed by the US government as a way for American companies to comply with European Union privacy laws.

NEW QUESTION 175
- (Exam Topic 3)
Most APIs will support a variety of different data formats or structures.
However, the SOAP API will only support which one of the following data formats?

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

Answer: A

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

NEW QUESTION 177
- (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 179
- (Exam Topic 3)
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 181
- (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 184
- (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 186
- (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 187
- (Exam Topic 3)
With IaaS, what is responsible for handling the security and control over the volume storage space?

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

Answer: B

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

NEW QUESTION 188
- (Exam Topic 3)
What type of storage structure does object storage employ to maintain files?

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

Answer: D

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

NEW QUESTION 189
- (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 192
- (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 193
- (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 197
- (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 202
- (Exam Topic 3)
You just hired an outside developer to modernize some applications with new web services and functionality. In order to implement a comprehensive test platform for validation, the developer needs a data set that resembles a production data set in both size and composition.
In order to accomplish this, what type of masking would you use?

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

Answer: C

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

NEW QUESTION 204
- (Exam Topic 3)
Different certifications and standards take different approaches to data center design and operations. Although many traditional approaches use a tiered methodology, which of the following utilizes a macro-level approach to data center design?

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

Answer: A

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

NEW QUESTION 207
- (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 209
- (Exam Topic 3)
Which cloud storage type resembles a virtual hard drive and can be utilized in the same manner and with the same type of features and capabilities?

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

Answer: A

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

NEW QUESTION 211
- (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 213
- (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 215
- (Exam Topic 2)
Which of the following is NOT a domain of the Cloud Controls Matrix (CCM)?

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

Answer: D

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

NEW QUESTION 217
- (Exam Topic 2)
Which crucial aspect of cloud computing can be most threatened by insecure APIs?

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

Answer: A

Explanation:
Cloud environments depend heavily on API calls for management and automation. Any vulnerability with the APIs can cause significant risk and exposure to all tenants of the cloud environment.

NEW QUESTION 220
- (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 224
- (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 226
- (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 229
- (Exam Topic 2)
Which approach is typically the most efficient method to use for data discovery?

A. Metadata
B. Content analysis
C. Labels
D. ACLs

Answer: A

Explanation:
Metadata is data about data. It contains information about the type of data, how it is stored and organized, or information about its creation and use.

NEW QUESTION 230
- (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 235
- (Exam Topic 2)
Which of the cloud deployment models requires the cloud customer to be part of a specific group or organization in order to host cloud services within it?

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

Answer: A

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

NEW QUESTION 238
- (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 241
- (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 246
- (Exam Topic 2)
Which audit type has been largely replaced by newer approaches since 2011?

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

Answer: C

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

NEW QUESTION 248
- (Exam Topic 2)
Which value refers to the percentage of production level restoration needed to meet BCDR objectives?

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

Answer: C

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

NEW QUESTION 253
- (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 258
- (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 261
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the ability to easily move services and applications between different cloud providers?

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

Answer: C

Explanation:
Portability is the ease with which a service or application can be moved between different cloud providers. Maintaining portability gives an organization great flexibility between cloud providers and the ability to shop for better deals or offerings.

NEW QUESTION 265
- (Exam Topic 2)
What process is used within a clustered system to provide high availability and load balancing?

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

Answer: D

Explanation:
Dynamic resource scheduling (DRS) is used within all clustering systems as the method for clusters to provide high availability, scaling, management, and workload distribution and balancing of jobs and processes. From a physical infrastructure perspective, DRS is used to balance compute loads between physical hosts in a cloud to maintain the desired thresholds and limits on the physical hosts.

NEW QUESTION 269
- (Exam Topic 2)
What type of data does data rights management (DRM) protect?

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

Answer: A

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

NEW QUESTION 273
- (Exam Topic 2)
The SOC Type 2 reports are divided into five principles.
Which of the five principles must also be included when auditing any of the other four principles?

A. Confidentiality
B. Privacy
C. Security
D. Availability

Answer: C

Explanation:
Under the SOC guidelines, when any of the four principles other than security are being audited, which includes availability, confidentiality, processing integrity, and privacy, the security principle must also be included with the audit.

NEW QUESTION 274
- (Exam Topic 2)
Which of the following technologies is used to monitor network traffic and notify if any potential threats or attacks are noticed?

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

Answer: D

Explanation:
An intrusion detection system (IDS) is designed to analyze network packets, compare their contents or characteristics against a set of configurations or signatures, and alert personnel if anything is detected that could constitute a threat or is otherwise designated for alerting.

NEW QUESTION 277
- (Exam Topic 2)
Which of the following is NOT one of five principles of SOC Type 2 audits?

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

Answer: C

Explanation:

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

NEW QUESTION 281
- (Exam Topic 2)
Which data point that auditors always desire is very difficult to provide within a cloud environment?

A. Access policy
B. Systems architecture
C. Baselines
D. Privacy statement

Answer: B

Explanation:
Cloud environments are constantly changing and often span multiple physical locations. A cloud customer is also very unlikely to have knowledge and insight into the underlying systems architecture in a cloud environment. Both of these realities make it very difficult, if not impossible, for an organization to provide a comprehensive systems design document.

NEW QUESTION 285
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the ability for a cloud customer to easily remove their applications and data from a cloud environment?

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

Answer: A

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

NEW QUESTION 289
- (Exam Topic 2)
Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?

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

Answer: A

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

NEW QUESTION 294
- (Exam Topic 2)
Which aspect of cloud computing makes data classification even more vital than in a traditional data center?

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

Answer: C

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

NEW QUESTION 297
- (Exam Topic 1)
What is the biggest concern with hosting a key management system outside of the cloud environment?

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

Answer: C

Explanation:
When a key management system is outside of the cloud environment hosting the application, availability is a primary concern because any access issues with the

encryption keys will render the entire application unusable.

NEW QUESTION 299
- (Exam Topic 1)
Which of the following publishes the most commonly used standard for data center design in regard to tiers and topologies?

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

Answer: B

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

NEW QUESTION 301
- (Exam Topic 1)
Which of the following roles is responsible for creating cloud components and the testing and validation of services?

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

Answer: D

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

NEW QUESTION 304
- (Exam Topic 1)
Which of the following would NOT be considered part of resource pooling with an Infrastructure as a Service implementation?

A. Storage
B. Application
C. Mamory
D. CPU

Answer: B

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

NEW QUESTION 307
- (Exam Topic 1)
What are the two protocols that TLS uses?

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

Answer: A

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

NEW QUESTION 311
- (Exam Topic 1)
Which of the following is NOT a criterion for data within the scope of eDiscovery?

A. Possession
B. Custody
C. Control
D. Archive

Answer: D

Explanation:
eDiscovery pertains to information and data that is in the possession, control, and custody of an organization.

NEW QUESTION 312

- (Exam Topic 1)
Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?

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

Answer: B

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

NEW QUESTION 315
- (Exam Topic 1)
Which of the following threat types can occur when an application does not properly validate input and can be leveraged to send users to malicious sites that appear to be legitimate?

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

Answer: A

Explanation:
Many web applications offer redirect or forward pages that send users to different, external sites. If these pages are not properly secured and validated, attackers can use the application to forward users off to sites for phishing or malware attempts. These attempts can often be more successful than direct phishing attempts because users will trust the site or application that sent them there, and they will assume it has been properly validated and approved by the trusted application's owners or operators. Security misconfiguration occurs when applications and systems are not properly configured for security--often a result of misapplied or inadequate baselines. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data.

NEW QUESTION 320
- (Exam Topic 1)
Which of the following actions will NOT make data part of the "create" phase of the cloud data lifecycle?

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

Answer: A

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

NEW QUESTION 322
- (Exam Topic 1)
Which type of audit report does many cloud providers use to instill confidence in their policies, practices, and procedures to current and potential customers?

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

Answer: B

Explanation:
One approach that many cloud providers opt to take is to undergo a SOC 2 audit and make the report available to cloud customers and potential cloud customers as a way of providing security confidence without having to open their systems or sensitive information to the masses.

NEW QUESTION 325
- (Exam Topic 1)
Which United States law is focused on PII as it relates to the financial industry?

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

Answer: D

Explanation:

The GLBA, as it is commonly called based on the lead sponsors and authors of the act, is officially known as "The Financial Modernization Act of 1999." It is specifically focused on PII as it relates to financial institutions. There are three specific components of it, covering various areas and use, on top of a general requirement that all financial institutions must provide all users and customers with a written copy of their privacy policies and practices, including with whom and for what reasons their information may be shared with other entities.

NEW QUESTION 327
- (Exam Topic 1)
Which of the following storage types is most closely associated with a database-type storage implementation?

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

Answer: D

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

NEW QUESTION 328
- (Exam Topic 1)
Which of the following is the optimal humidity level for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?

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

Answer: D

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

NEW QUESTION 332
- (Exam Topic 1)
What is the data encapsulation used with the SOAP protocol referred to?

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

Answer: B

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

NEW QUESTION 337
- (Exam Topic 1)
Which term relates to the application of scientific methods and practices to evidence?

A. Forensics
B. Methodical
C. Theoretical
D. Measured

Answer: A

Explanation:
Forensics is the application of scientific and methodical processes to identify, collect, preserve, analyze, and summarize/report digital information and evidence.

NEW QUESTION 341
- (Exam Topic 1)
Which of the following is the optimal temperature for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?

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

Answer: B

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

NEW QUESTION 346
- (Exam Topic 1)
Which of the following roles involves the connection and integration of existing systems and services to a cloud environment?

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

Answer: D

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

NEW QUESTION 348
- (Exam Topic 1)
Which of the following standards primarily pertains to cabling designs and setups in a data center?

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

Answer: B

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

NEW QUESTION 353
- (Exam Topic 1)
Which United States program was designed to enable organizations to bridge the gap between privacy laws and requirements of the United States and the European Union?

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

Answer: C

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

NEW QUESTION 354
- (Exam Topic 1)
Which of the following roles is responsible for overseeing customer relationships and the processing of financial transactions?

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

Answer: C

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

NEW QUESTION 359
- (Exam Topic 1)
Which concept BEST describes the capability for a cloud environment to automatically scale a system or application, based on its current resource demands?

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

Answer: D

Explanation:
Rapid elasticity allows a cloud environment to automatically add or remove resources to or from a system or application based on its current demands. Whereas a traditional data center model would require standby hardware and substantial effort to add resources in response to load increases, a cloud environment can easily and rapidly expand to meet resources demands, so long as the application is properly implemented for it.

NEW QUESTION 363
- (Exam Topic 1)
What is the primary reason that makes resolving jurisdictional conflicts complicated?

A. Different technology standards
B. Costs
C. Language barriers
D. Lack of international authority

Answer: D

Explanation:
With international operations, systems ultimately cross many jurisdictional boundaries, and many times, they conflict with each other. The major hurdle to overcome for an organization is the lack of an ultimate international authority to mediate such conflicts, with a likely result of legal efforts in each jurisdiction.

NEW QUESTION 365
- (Exam Topic 1)
Which aspect of cloud computing will be most negatively impacted by vendor lock-in?

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

Answer: D

Explanation:
A cloud customer utilizing proprietary APIs or services from one cloud provider that are unlikely to be available from another cloud provider will most negatively impact portability.

NEW QUESTION 370
- (Exam Topic 1)
Which type of cloud model typically presents the most challenges to a cloud customer during the "destroy" phase of the cloud data lifecycle?

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

Answer: C

Explanation:
With many SaaS implementations, data is not isolated to a particular customer but rather is part of the overall application. When it comes to data destruction, a particular challenge is ensuring that all of a customer's data is completely destroyed while not impacting the data of other customers.

NEW QUESTION 374
- (Exam Topic 1)
What is the only data format permitted with the SOAP API?

A. HTML
B. SAML
C. XSML
D. XML

Answer: D

Explanation:
The SOAP protocol only supports the XML data format.

NEW QUESTION 379
- (Exam Topic 1)
Which of the following is considered an internal redundancy for a data center?

A. Power distribution units
B. Network circuits
C. Power substations
D. Generators

Answer: A

Explanation:
Power distribution units are internal to a data center and supply power to internal components such as racks, appliances, and cooling systems. As such, they are considered an internal redundancy.

NEW QUESTION 383
- (Exam Topic 1)

Which of the following concepts refers to a cloud customer paying only for the resources and offerings they use within a cloud environment, and only for the duration that they are consuming them?

A. Consumable service
B. Measured service
C. Billable service
D. Metered service

Answer: B

Explanation:
Measured service is where cloud services are delivered and billed in a metered way, where the cloud customer only pays for those that they actually use, and for the duration of time that they use them.

NEW QUESTION 387
- (Exam Topic 1)
How is an object stored within an object storage system?

A. Key value
B. Database
C. LDAP
D. Tree structure

Answer: A

Explanation:
Object storage uses a flat structure with key values to store and access objects.

NEW QUESTION 392
- (Exam Topic 1)
Which of the following storage types is most closely associated with a traditional file system and tree structure?

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

Answer: A

Explanation:
Volume storage works as a virtual hard drive that is attached to a virtual machine. The operating system sees the volume the same as how a traditional drive on a physical server would be seen.

NEW QUESTION 394
- (Exam Topic 1)
Which of the following is considered an external redundancy for a data center?

A. Power feeds to rack
B. Generators
C. Power distribution units
D. Storage systems

Answer: B

Explanation:
Generators are considered an external redundancy to a data center. Power distribution units (PDUs), storage systems, and power feeds to racks are all internal to a data center, and as such they are considered internal redundancies.

NEW QUESTION 397
- (Exam Topic 1)
Which of the following threat types involves an application that does not validate authorization for portions of itself after the initial checks?

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

Answer: B

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

NEW QUESTION 401
- (Exam Topic 1)
Which of the following security technologies is commonly used to give administrators access into trust zones within an environment?

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

Answer: A

Explanation:
Virtual private networks (VPNs) are commonly used to allow access into trust zones. Via a VPN, access can be controlled and logged and only allowed through secure channels by authorized users. It also adds an additional layer of encryption and protection to communications.

NEW QUESTION 406
- (Exam Topic 1)
What is used for local, physical access to hardware within a data center?

A. SSH
B. KVM
C. VPN
D. RDP

Answer: B

Explanation:
Local, physical access in a data center is done via KVM (keyboard, video, mouse) switches.

NEW QUESTION 410
......