ISC2

Exam Questions CCSP

Certified Cloud Security Professional

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

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

Answer: B

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

NEW QUESTION 2
- (Exam Topic 4)
Which of the following is considered a physical control?

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

Answer: A

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

NEW QUESTION 3
- (Exam Topic 4)
Countermeasures for protecting cloud operations against external attackers include all of the following except:

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

Answer: B

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

NEW QUESTION 4
- (Exam Topic 4)
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 cloud service category most commonly uses client-side key management systems?

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

Answer: A

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

cloud provider.

NEW QUESTION 6
- (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 7
- (Exam Topic 4)
What type of masking would you employ to produce a separate data set for testing purposes based on production data without any sensitive information?

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

Answer: D

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

NEW QUESTION 8
- (Exam Topic 4)
Which ITIL component focuses on ensuring that system resources, processes, and personnel are properly allocated to meet SLA requirements?

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

Answer: B

Explanation:
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. Configuration management tracks and maintains detailed information about all IT components within an organization. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION 9
- (Exam Topic 4)
Which of the following provides assurance, to a predetermined acceptable level of certainty, that an entity is indeed who they claim to be?

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

Answer: A

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

NEW QUESTION 10
- (Exam Topic 4)
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)
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 11
- (Exam Topic 4)
Which of the following best describes the Organizational Normative Framework (ONF)?

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

Answer: D

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

NEW QUESTION 13
- (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 16
- (Exam Topic 4)
Which data sanitation method is also commonly referred to as "zeroing"?

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

Answer: A

Explanation:
The zeroing of data--or the writing of null values or arbitrary data to ensure deletion has been fully completed--is officially referred to as overwriting. Nullification, deleting, and blanking are provided as distractor terms.

NEW QUESTION 18
- (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 20
- (Exam Topic 4)
The WS-Security standards are built around all of the following standards except which one?

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

Answer: A

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

NEW QUESTION 22
- (Exam Topic 4)
Database activity monitoring (DAM) can be:

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

Answer: A

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

NEW QUESTION 23
- (Exam Topic 4)
DLP solutions can aid in deterring loss due to which of the following?

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

Answer: C

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 27
- (Exam Topic 4)
All the following are data analytics modes, except:

A. Datamining
B. Agile business intelligence
C. Refractory iterations
D. Real-time analytics

Answer: C

Explanation:
All the others are data analytics methods, but “refractory iterations” is a nonsense term thrown in as a red herring.

NEW QUESTION 32
- (Exam Topic 4)
Limits for resource utilization can be set at different levels within a cloud environment to ensure that no particular entity can consume a level of resources that impacts other cloud customers.
Which of the following is NOT a unit covered by limits?

A. Hypervisor
B. Cloud customer
C. Virtual machine
D. Service

Answer: A

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

NEW QUESTION 36
- (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 37
- (Exam Topic 4)
Which component of ITIL involves planning for the restoration of services after an unexpected outage or incident?

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

Answer: A

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

NEW QUESTION 40
- (Exam Topic 4)
IRM solutions allow an organization to place different restrictions on data usage than would otherwise be possible through traditional security controls.
Which of the following controls would be possible with IRM that would not with traditional security controls?

A. Copy
B. Read
C. Delete
D. Print

Answer: D

Explanation:
Traditional security controls would not be able to restrict a user from printing something that they have the ability to access and read, but IRM solutions would allow for such a restriction. If a user has permissions to read a file, he can also copy the file or print it under traditional controls, and the ability to modify or write will give the user the ability to delete.

NEW QUESTION 41
- (Exam Topic 4)
Hardening the operating system refers to all of the following except:

A. Limiting administrator access
B. Closing unused ports
C. Removing antimalware agents
D. Removing unnecessary services and libraries

Answer: C

Explanation:
Removing antimalware agents. Hardening the operating system means making it more secure. Limiting administrator access, closing unused ports, and removing unnecessary services and libraries all have the potential to make an OS more secure. But removing antimalware agents would actually make the system less secure. If anything, antimalware agents should be added, not removed.

NEW QUESTION 43
- (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 44
- (Exam Topic 4)
What's a potential problem when object storage versus volume storage is used within IaaS for application use and dependency?

A. Object storage is only optimized for small files.
B. Object storage is its own system, and data consistency depends on replication.
C. Object storage may have availability issues.
D. Object storage is dependent on access control from the host server.

Answer: B

Explanation:
Object storage runs on its own independent systems, which have their own redundancy and distribution. To ensure data consistency, sufficient time is needed for objects to fully replicate to all potential locations before being accessed. Object storage is optimized for high availability and will not be any less reliable than any other virtual machine within a cloud environment. It is hosted on a separate system that does not have dependencies in local host servers for access control, and it is optimized for files of all different sizes and uses.

NEW QUESTION 46
- (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 48
- (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 49
- (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 52
- (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 53
- (Exam Topic 4)
What is a key capability or characteristic of PaaS?

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

Answer: C

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

NEW QUESTION 55
- (Exam Topic 4)
When using a PaaS solution, what is the capability provided to the customer?

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

Answer: B

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

NEW QUESTION 57
- (Exam Topic 4)
Above and beyond general regulations for data privacy and protection, certain types of data are subjected to more rigorous regulations and oversight.
Which of the following is not a regulatory framework for more sensitive or specialized data?

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

Answer: A

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

NEW QUESTION 62
- (Exam Topic 4)
What is the experimental technology that might lead to the possibility of processing encrypted data without having to decrypt it first?

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

Answer: D

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

NEW QUESTION 66
- (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 71
- (Exam Topic 4)
Proper implementation of DLP solutions for successful function requires which of the following?

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

Answer: C

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

NEW QUESTION 75
- (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 80
- (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 81
- (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 84
- (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)
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 90
- (Exam Topic 4)
When using an IaaS solution, what is a key benefit provided to the customer?

A. Metered and priced on the basis of units consumed
B. Increased energy and cooling system efficiencies
C. Transferred cost of ownership
D. The ability to scale up infrastructure services based on projected usage

Answer: A

Explanation:
IaaS has a number of key benefits for organizations, which include but are not limited to these: -- - Usage is metered and priced on the basis of units (or instances) consumed. This can also be billed back to specific departments or functions.
- It has an ability to scale up and down infrastructure services based on actual usage. This is particularly useful and beneficial where there are significant spikes and dips within the usage curve for infrastructure.
- It has a reduced cost of ownership. There is no need to buy assets for everyday use, no loss of asset value over time, and reduced costs of maintenance and support.
- It has a reduced energy and cooling costs along with “green IT” environment effect with optimum use of IT resources and systems.

NEW QUESTION 93
- (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 97
- (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 102
- (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 103
- (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 105
- (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 107
- (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 112
- (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 113
- (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 117
- (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 121
- (Exam Topic 4)
BCDR strategies do not typically involve the entire operations of an organization, but only those deemed critical to their business.

Which concept pertains to the amount of services that need to be recovered to meet BCDR objectives?

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

Answer: A

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

NEW QUESTION 124
- (Exam Topic 4)
Countermeasures for protecting cloud operations against internal threats include all of the following except:

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

Answer: D

Explanation:
Conflict of interest is a threat, not a control.

NEW QUESTION 127
- (Exam Topic 4)
What must SOAP rely on for security since it does not provide security as a built-in capability?

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

Answer: A

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

NEW QUESTION 132
- (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 133
- (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 135
- (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 138
- (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 141
- (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 143
- (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 147
- (Exam Topic 4)
Which of the following is the primary purpose of an SOC 3 report?

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

Answer: C

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

NEW QUESTION 149
- (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 152
- (Exam Topic 4)
Which of the following best describes a sandbox?

A. An isolated space where untested code and experimentation can safely occur separate from the production environment.
B. A space where you can safely execute malicious code to see what it does.
C. An isolated space where transactions are protected from malicious software
D. An isolated space where untested code and experimentation can safely occur within the production environment.

Answer: A

Explanation:
Options C and B are also correct, but A is more general and incorporates them both. D is incorrect, because sandboxing does not take place in the production environment.

NEW QUESTION 154
- (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 156
- (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 161
- (Exam Topic 3)
You are working for a cloud service provider and receive an eDiscovery order pertaining to one of your customers. Which of the following would be the most appropriate action to take first?

A. Take a shapshot of the virtual machines
B. Escrow the encryption keys
C. Copy the data
D. Notify the customer

Answer: D

Explanation:
When a cloud service provider receives an eDiscovery order pertaining to one of their customers, the first action they must take is to notify the customer. This allows the customer to be aware of what was received, as well as to conduct a review to determine if any challenges are necessary or warranted. Taking snapshots of virtual machines, copying data, and escrowing encryption keys are all processes involved in the actual collection of data and should not be performed until the customer has been notified of the request.

NEW QUESTION 163
- (Exam Topic 3)
What is a serious complication an organization faces from the compliance perspective with international operations?

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

Answer: A

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

NEW QUESTION 164
- (Exam Topic 3)
Which of the following is considered an internal redundancy for a data center?

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

Answer: B

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

NEW QUESTION 165
- (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 169
- (Exam Topic 3)
Data centers have enormous power resources that are distributed and consumed throughout the entire facility. Which of the following standards pertains to the proper fire safety standards within that scope?

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

Answer: C

Explanation:
The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers. The International Data Center Authority (IDCA) offers the Infinity Paradigm, which takes a macro-level approach to data center design.

NEW QUESTION 171
- (Exam Topic 3)
If a cloud computing customer wishes to guarantee that a minimum level of resources will always be available, which of the following set of services would

compromise the reservation?

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

Answer: D

Explanation:
A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources.
A reservation pertains to memory and CPU resources. Under the concept of a reservation, memory and CPU are the guaranteed resources, but storage and networking are not included even though they are core components of cloud computing. Software would be out of scope for a guarantee and doesn't really pertain to the concept.

NEW QUESTION 173
- (Exam Topic 3)
Which cloud service category would be most ideal for a cloud customer that is developing software to test its applications among multiple hosting providers to determine the best option for its needs?

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

Answer: B

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

NEW QUESTION 176
- (Exam Topic 3)
For service provisioning and support, what is the ideal amount of interaction between a cloud customer and cloud provider?

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

Answer: C

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

NEW QUESTION 177
- (Exam Topic 3)
Although host-based and network-based IDSs perform similar functions and have similar capabilities, which of the following is an advantage of a network-based IDS over a host-based IDS, assuming all capabilities are equal?

A. Segregated from host systems
B. Network access
C. Scalability
D. External to system patching

Answer: A

Explanation:
A network-based IDS has the advantage of being segregated from host systems, and as such, it would not be open to compromise in the same manner a host-based system would be. Although a network-based IDS would be external to system patching, this is not the best answer here because it is a minor concern compared to segregation due to possible host compromise. Scalability is also not the best answer because, although a network-based IDS does remove processing from the host system, it is not a primary security concern. Network access is not a consideration because both a host-based IDS and a network-based IDS would have access to network resources.

NEW QUESTION 178
- (Exam Topic 3)
Which cloud storage type is typically used to house virtual machine images that are used throughout the environment?

A. Structured
B. Unstructured
C. Volume

D. Object

Answer: D

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

NEW QUESTION 179
- (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 182
- (Exam Topic 3)
Within a federated identity system, which of the following would you be MOST likely to use for sending information for consumption by a relying party?

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

Answer: D

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

NEW QUESTION 183
- (Exam Topic 3)
Which of the following actions will NOT make data part of the create phase of the cloud data lifecycle?

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

Answer: B

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

NEW QUESTION 185
- (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 189
- (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 194
- (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 199
- (Exam Topic 3)
Along with humidity, temperature is crucial to a data center for optimal operations and protection of equipment.
Which of the following is the optimal temperature range as set by ASHRAE?

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

Answer: C

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

NEW QUESTION 204
- (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 206
- (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 208
- (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 213
- (Exam Topic 3)
Within a SaaS environment, what is the responsibility on the part of the cloud customer in regard to procuring the software used?

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

Answer: B

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

NEW QUESTION 214
- (Exam Topic 3)
ISO/IEC has established international standards for many aspects of computing and any processes or procedures related to information technology.
Which ISO/IEC standard has been established to provide a framework for handling eDiscovery processes?

A. ISO/IEC 27001
B. ISO/IEC 27002
C. ISO/IEC 27040
D. ISO/IEC 27050

Answer: D

Explanation:
ISO/IEC 27050 strives to establish an internationally accepted standard for eDiscovery processes and best practices. It encompasses all steps of the eDiscovery process, including the identification, preservation, collection, processing, review, analysis, and the final production of the requested data archive. ISO/IEC 27001 is a general security specification for an information security management system. ISO/IEC 27002 gives best practice recommendations for information security management. ISO/IEC 27040 is focused on the security of storage systems.

NEW QUESTION 218
- (Exam Topic 3)
You were recently hired as a project manager at a major university to implement cloud services for the academic and administrative systems. Because the load and demand for services at a university are very cyclical in nature, commensurate with the academic calendar, which of the following aspects of cloud computing would NOT be a primary benefit to you?

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

Answer: B

Explanation:
Broad network access to cloud services, although it is an integral aspect of cloud computing, would not being a specific benefit to an organization with cyclical business needs. The other options would allow for lower costs during periods of low usage as well as provide the ability to expand services quickly and easily when needed for peak periods. Measured service allows a cloud customer to only use the resources it needs at the time, and resource pooling allows a cloud customer to access resources as needed. On-demand self-service enables the cloud customer to change its provisioned resources on its own, without the need to interact with the staff from the cloud provider.

NEW QUESTION 221

- (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 226
- (Exam Topic 3)
Implementing baselines on systems would take an enormous amount of time and resources if the staff had to apply them to each server, and over time, it would be almost impossible to keep all the systems in sync on an ongoing basis.
Which of the following is NOT a package that can be used for implementing and maintaining baselines across an enterprise?

A. Puppet
B. SCCM
C. Chef
D. GitHub

Answer: D

Explanation:
GitHub is a software development platform that serves as a code repository and versioning system. It is solely used for software development and would not be appropriate for applying baselines to systems. Puppet is an open-source configuration management tool that runs on many platforms and can be used to apply and maintain baselines. The Software Center Configuration Manager (SCCM) was developed by Microsoft for managing systems across large groups of servers. Chef is also a system for maintaining large groups of systems throughout an enterprise.

NEW QUESTION 231
- (Exam Topic 3)
With an API, various features and optimizations are highly desirable to scalability, reliability, and security. What does the REST API support that the SOAP API does NOT support?

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

Answer: B

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

NEW QUESTION 232
- (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 236
- (Exam Topic 3)
Which phase of the cloud data lifecycle represents the first instance where security controls can be implemented?

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

Answer: C

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

NEW QUESTION 240
- (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 242
- (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 246
- (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 247
- (Exam Topic 2)
Which of the cloud deployment models offers the easiest initial setup and access for the cloud customer?

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

Answer: D

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

NEW QUESTION 249
- (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 250
- (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 254
- (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 258
- (Exam Topic 2)
Which value refers to the amount of time it takes to recover operations in a BCDR situation to meet management's objectives?

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

Answer: D

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

NEW QUESTION 263
- (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 268
- (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 270

- (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 272
- (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 277
- (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 279
- (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 280
- (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 281
- (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 283
- (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 287
- (Exam Topic 2)
Which regulatory system pertains to the protection of healthcare data?

A. HIPAA
B. HAS
C. HITECH
D. HFCA

Answer: A

Explanation:
The Health Insurance Portability and Accountability Act (HIPAA) sets stringent requirements in the United States for the protection of healthcare records.

NEW QUESTION 291
- (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 296
- (Exam Topic 2)
Which of the following would be a reason to undertake a BCDR test?

A. Functional change of the application
B. Change in staff
C. User interface overhaul of the application
D. Change in regulations

Answer: A

Explanation:
Any time a major functional change of an application occurs, a new BCDR test should be done to ensure the overall strategy and process are still applicable and appropriate.

NEW QUESTION 298
- (Exam Topic 2)
Which attribute of data poses the biggest challenge for data discovery?

A. Labels

B. Quality
C. Volume
D. Format

Answer: B

Explanation:
The main problem when it comes to data discovery is the quality of the data that analysis is being performed against. Data that is malformed, incorrectly stored or labeled, or incomplete makes it very difficult to use analytical tools against.

NEW QUESTION 299
- (Exam Topic 2)
Which of the following should NOT be part of the requirement analysis phase of the software development lifecycle?

A. Functionality
B. Programming languages
C. Software platform
D. Security requirements

Answer: D

Explanation:
Security requirements should be incorporated into the software development lifecycle (SDLC) from the earliest requirement gathering stage and should be incorporated prior to the requirement analysis phase.

NEW QUESTION 300
- (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 305
- (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 310
- (Exam Topic 2)
Which of the following is NOT something that an HIDS will monitor?

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

Answer: B

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

NEW QUESTION 312
- (Exam Topic 2)
Which security concept is focused on the trustworthiness of data?

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

Answer: A

Explanation:
Integrity is focused on the trustworthiness of data as well as the prevention of unauthorized modification or tampering of it. A prime consideration for maintaining integrity is an emphasis on the change management and configuration management aspects of operations, so that all modifications are predictable, tracked, logged, and verified, whether they are performed by actual human users or systems processes and scripts.

NEW QUESTION 314
- (Exam Topic 2)
What is the minimum regularity for testing a BCDR plan to meet best practices?

A. Once year
B. Once a month
C. Every six months
D. When the budget allows it

Answer: A

Explanation:
Best practices and industry standards dictate that a BCDR solution should be tested at least once a year, though specific regulatory requirements may dictate more regular testing. The BCDR plan should also be tested whenever a major modification to a system occurs.

NEW QUESTION 315
- (Exam Topic 2)
What concept does the "R" represent with the DREAD model?

A. Reproducibility
B. Repudiation
C. Risk
D. Residual

Answer: A

Explanation:
Reproducibility is the measure of how easy it is to reproduce and successful use an exploit. Scoring within the DREAD model ranges from 0, signifying a nearly impossibly exploit, up to 10, which signifies something that anyone from a simple function call could exploit, such as a URL.

NEW QUESTION 320
- (Exam Topic 1)
What type of PII is controlled based on laws and carries legal penalties for noncompliance with requirements?

A. Contractual
B. Regulated
C. Specific
D. Jurisdictional

Answer: B

Explanation:
Regulated PII involves those requirements put forth by specific laws or regulations, and unlike contractual PII, where a violation can lead to contractual penalties, a violation of regulated PII can lead to fines or even criminal charges in some jurisdictions. PII regulations can depend on either the jurisdiction that applies to the hosting location or application or specific legislation based on the industry or type of data used.

NEW QUESTION 322
- (Exam Topic 1)
Which of the following may unilaterally deem a cloud hosting model inappropriate for a system or application?

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

Answer: C

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

NEW QUESTION 326
- (Exam Topic 1)
From a legal perspective, what is the most important first step after an eDiscovery order has been received by the cloud provider?

A. Notification
B. Key identification
C. Data collection
D. Virtual image snapshots

Answer: A

Explanation:
The contract should include requirements for notification by the cloud provider to the cloud customer upon the receipt of such an order. This serves a few important purposes. First, it keeps communication and trust open between the cloud provider and cloud customers. Second, and more importantly, it allows the cloud customer to potentially challenge the order if they feel they have the grounds or desire to do so.

NEW QUESTION 331
- (Exam Topic 1)
Which aspect of archiving must be tested regularly for the duration of retention requirements?

A. Availability
B. Recoverability
C. Auditability
D. Portability

Answer: B

Explanation:
In order for any archiving system to be deemed useful and compliant, regular tests must be performed to ensure the data can still be recovered and accessible, should it ever be needed, for the duration of the retention requirements.

NEW QUESTION 334
- (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 335
- (Exam Topic 1)
Which of the following attempts to establish an international standard for eDiscovery processes and best practices?

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

Answer: B

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

NEW QUESTION 337
- (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 342
- (Exam Topic 1)
What is the biggest negative to leasing space in a data center versus building or maintain your own?

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

Answer: B

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

NEW QUESTION 345
- (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 348
- (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 353
- (Exam Topic 1)
Which of the following threat types can occur when baselines are not appropriately applied or unauthorized changes are made?

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

Answer: C

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

NEW QUESTION 354
- (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 358
- (Exam Topic 1)
What type of PII is regulated based on the type of application or per the conditions of the specific hosting agreement?

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

Answer: B

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

NEW QUESTION 361
- (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 363
- (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 366
- (Exam Topic 1)
Why does a Type 1 hypervisor typically offer tighter security controls than a Type 2 hypervisor?

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

Answer: B

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

NEW QUESTION 368
- (Exam Topic 1)
Which of the following pertains to fire safety standards within a data center, specifically with their enormous electrical consumption?

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

Answer: A

Explanation:
The standards put out by the National Fire Protection Association (NFPA) cover general fire protection best practices for any type of facility, but also specific publications pertaining to IT equipment and data centers.

NEW QUESTION 371
- (Exam Topic 1)
What does the management plane typically utilize to perform administrative functions on the hypervisors that it has access to?

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

Answer: C

Explanation:

The functions of the management plane are typically exposed as a series of remote calls and function executions and as a set of APIs. These APIs are typically leveraged through either a client or a web portal, with the latter being the most common.

NEW QUESTION 373
- (Exam Topic 1)
Which of the following represents a minimum guaranteed resource within a cloud environment for the cloud customer?

A. Reservation
B. Share
C. Limit
D. Provision

Answer: A

Explanation:
A reservation is a minimum resource that is guaranteed to a customer within a cloud environment. Within a cloud, a reservation can pertain to the two main aspects of computing: memory and processor. With a reservation in place, the cloud provider guarantees that a cloud customer will always have at minimum the necessary resources available to power on and operate any of their services.

NEW QUESTION 374
- (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 377
- (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 382
- (Exam Topic 1)
Which technique involves replacing values within a specific data field to protect sensitive data?

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

Answer: B

Explanation:
Masking involves replacing specific data within a data set with new values. For example, with credit card fields, as most who have ever purchased anything online can attest, nearly the entire credit card number is masked with a character such as an asterisk, with the last four digits left visible for identification and confirmation.

NEW QUESTION 386
- (Exam Topic 1)
Which of the following roles involves overseeing billing, purchasing, and requesting audit reports for an organization within a cloud environment?

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

Answer: B

Explanation:
The cloud service business manager is responsible for overseeing business and billing administration, purchasing cloud services, and requesting audit reports when necessary

NEW QUESTION 389
- (Exam Topic 1)
Which of the following roles is responsible for obtaining new customers and securing contracts and agreements?

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

Answer: B

Explanation:
The cloud service broker is responsible for obtaining new customers, analyzing the marketplace, and securing contracts and agreements.

NEW QUESTION 393
- (Exam Topic 1)
What is a serious complication an organization faces from the perspective of compliance with international operations?

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

Answer: B

Explanation:
When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, and many times they might be in contention with one other or not clearly applicable. These requirements can include the location of the users and the type of data they enter into systems, the laws governing the organization that owns the application and any regulatory requirements they may have, as well as the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which might be multiple jurisdictions as well.

NEW QUESTION 395
- (Exam Topic 1)
Which networking concept in a cloud environment allows for network segregation and isolation of IP spaces?

A. PLAN
B. WAN
C. LAN
D. VLAN

Answer: D

Explanation:
A virtual area network (VLAN) allows the logical separation and isolation of networks and IP spaces to provide enhanced security and controls.

NEW QUESTION 400
- (Exam Topic 1)
Which of the following roles involves the provisioning and delivery of cloud services?

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

Answer: C

Explanation:
The cloud service manager is responsible for the delivery of cloud services, the provisioning of cloud services, and the overall management of cloud services.

NEW QUESTION 401
- (Exam Topic 1)
Which of the following roles involves testing, monitoring, and securing cloud services for an organization?

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

Answer: D

Explanation:
The cloud service administrator is responsible for testing cloud services, monitoring services, administering security for services, providing usage reports on cloud services, and addressing problem reports

NEW QUESTION 405
- (Exam Topic 1)
Which of the following threat types can occur when encryption is not properly applied or insecure transport mechanisms are used?

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

Answer: C

Explanation:
Sensitive data exposure occurs when information is not properly secured through encryption and secure transport mechanisms; it can quickly become an easy and broad method for attackers to compromise information. Web applications must enforce strong encryption and security controls on the application side, but secure methods of communications with browsers or other clients used to access the information are also required. 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. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, thus allowing spoofing for malware or phishing attacks.

NEW QUESTION 407
- (Exam Topic 1)
Which of the following security measures done at the network layer in a traditional data center are also applicable to a cloud environment?

A. Dedicated switches
B. Trust zones
C. Redundant network circuits
D. Direct connections

Answer: B

Explanation:
Trust zones can be implemented to separate systems or tiers along logical lines for great security and access controls. Each zone can then have its own security controls and monitoring based on its particular needs.

NEW QUESTION 409
- (Exam Topic 1)
What does the REST API support that SOAP does NOT support?

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

Answer: A

Explanation:
The SOAP protocol does not support caching, whereas the REST API does.

NEW QUESTION 412
- (Exam Topic 1)
Which technology can be useful during the "share" phase of the cloud data lifecycle to continue to protect data as it leaves the original system and security controls?

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

Answer: C

Explanation:
Data loss prevention (DLP) can be applied to data that is leaving the security enclave to continue to enforce access restrictions and policies on other clients and systems.

NEW QUESTION 415
- (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 417
- (Exam Topic 1)
What is the best source for information about securing a physical asset's BIOS?

A. Security policies
B. Manual pages
C. Vendor documentation
D. Regulations

Answer: C

Explanation:
Vendor documentation from the manufacturer of the physical hardware is the best source of best practices for securing the BIOS.

NEW QUESTION 421
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CCSP Practice Exam Features:

* CCSP Questions and Answers Updated Frequently

* CCSP Practice Questions Verified by Expert Senior Certified Staff

* CCSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

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