Exam Questions CCSP

Certified Cloud Security Professional

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

NEW QUESTION 1
- (Exam Topic 4)
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the required amount of time to restore services to the predetermined level?

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

Answer: C

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

NEW QUESTION 2
- (Exam Topic 4)
APIs are defined as which of the following?

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

Answer: B

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

NEW QUESTION 3
- (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 4
- (Exam Topic 4)
A data custodian is responsible for which of the following?

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

Answer: C

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

NEW QUESTION 5
- (Exam Topic 4)
Data labels could include all the following, except:

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

Answer: A

Explanation:
All the others might be included in data labels, but we don’t usually include data value, since it is prone to change frequently, and because it might not be

information we want to disclose to anyone who does not have need to know.

NEW QUESTION 6
- (Exam Topic 4)
Countermeasures for protecting cloud operations against internal threats include all of the following except:

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

Answer: C

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

NEW QUESTION 7
- (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 8
- (Exam Topic 4)
Tokenization requires two distinct ________.

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

Answer: D

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

NEW QUESTION 9
- (Exam Topic 4)
In addition to battery backup, a UPS can offer which capability?

A. Breach alert
B. Confidentiality
C. Communication redundancy
D. Line conditioning

Answer: D

Explanation:
A UPS can provide line conditioning, adjusting power so that it is optimized for the devices it serves and smoothing any power fluctuations; it does not offer any of the other listed functions.

NEW QUESTION 10
- (Exam Topic 4)
Which 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 10
- (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 14
- (Exam Topic 4)
Which component of ITIL involves handling anything that can impact services for either internal or public users?

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

Answer: A

Explanation:

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

NEW QUESTION 16
- (Exam Topic 4)
As a result of scandals involving publicly traded corporations such as Enron, WorldCom, and Adelphi, Congress passed legislation known as:

A. SOX
B. HIPAA
C. FERPA
D. GLBA

Answer: A

Explanation:
Sarbanes-Oxley was a direct response to corporate scandals. FERPA is related to education. GLBA is about the financial industry. HIPAA is about health care.

NEW QUESTION 18
- (Exam Topic 4)
Deviations from the baseline should be investigated and _______.

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

Answer: B

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

NEW QUESTION 22
- (Exam Topic 4)
Which of the following jurisdictions lacks a comprehensive national policy on data privacy and the protection of personally identifiable information (PII)?

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

Answer: C

Explanation:
The United States has a myriad of regulations focused on specific types of data, such as healthcare and financial, but lacks an overall comprehensive privacy law

on the national level. The European Union, the Asian-Pacific Economic Cooperation, and Russia all have national privacy protections and regulations for the handling the PII data of their citizens.

NEW QUESTION 24
- (Exam Topic 4)
The different cloud service models have varying levels of responsibilities for functions and operations depending with the model's level of service.
In which of the following models would the responsibility for patching lie predominantly with the cloud customer?

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

Answer: D

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

NEW QUESTION 26
- (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 30
- (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 35
- (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 36
- (Exam Topic 4)
What does static application security testing (SAST) offer as a tool to the testers that makes it unique compared to other common security testing methodologies?

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

Answer:

B

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

NEW QUESTION 41
- (Exam Topic 4)
Cryptographic keys should be secured ________.

A. To a level at least as high as the data they can decrypt
B. In vaults
C. With two-person integrity
D. By armed guards

Answer: A

Explanation:
The physical security of crypto keys is of some concern, but guards or vaults are not always necessary.
Two-person integrity might be a good practice for protecting keys. The best answer to this question is option A, because it is always true, whereas the remaining options depend on circumstances.

NEW QUESTION 43
- (Exam Topic 4)
What masking strategy involves the replacing of sensitive data at the time it is accessed and used as it flows between the data and application layers of a service?

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

Answer: C

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

NEW QUESTION 46
- (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 51
- (Exam Topic 4)
Which format is the most commonly used standard for exchanging information within a federated identity system?

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

Answer: C

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

NEW QUESTION 56
- (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 58
- (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 61
- (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 63
- (Exam Topic 4)
Which protocol, as a part of TLS, handles negotiating and establishing a connection between two parties?

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

Answer: D

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

NEW QUESTION 67
- (Exam Topic 4)
DLP can be combined with what other security technology to enhance data controls?

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

Answer: A

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

NEW QUESTION 71
- (Exam Topic 4)
Apart from using encryption at the file system level, what technology is the most widely used to protect data stored in an object storage system?

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

Answer: D

Explanation:
Information rights management (IRM) technologies allow security controls and policies to be enforced on a data object regardless of where it resides. They also allow for extended controls such as expirations and copying restrictions, which are not available through traditional control mechanisms. Hypertext Transfer Protocol Secure (HTTPS), virtual private network (VPN), and Transport Layer Security (TLS) are all technologies and protocols that are widely used with cloud implementations for secure access to systems and services and likely will be used in conjunction with other object data protection strategies.

NEW QUESTION 73
- (Exam Topic 4)
What are SOC 1/SOC 2/SOC 3?

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

Answer: A

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

NEW QUESTION 75
- (Exam Topic 4)
What are third-party providers of IAM functions for the cloud environment?

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

Answer: D

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

NEW QUESTION 78
- (Exam Topic 4)
On large distributed systems with pooled resources, cloud computing relies on extensive orchestration to maintain the environment and the constant provisioning of resources.
Which of the following is crucial to the orchestration and automation of networking resources within a cloud?

A. DNSSEC
B. DNS
C. DCOM
D. DHCP

Answer: D

Explanation:
The Dynamic Host Configuration Protocol (DHCP) automatically configures network settings for a host so that these settings do not need to be configured on the host statically. Given the rapid and programmatic provisioning of resources within a cloud environment, this capability is crucial to cloud operations. Both DNS and its security-integrity extension DNSSEC provide name resolution to IP addresses, but neither is used for the configuration of network settings on a host. DCOM refers to the Distributed Component Object Model, which was developed by Microsoft as a means to request services across a network, and is not used for network configurations at all.

NEW QUESTION 79
- (Exam Topic 4)
DLP solutions can aid in deterring loss due to which of the following?

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

Answer: D

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

NEW QUESTION 83
- (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 88
- (Exam Topic 4)
Which of the following statements about Type 1 hypervisors is true?

A. The hardware vendor and software vendor are different.
B. The hardware vendor and software vendor are the same
C. The hardware vendor provides an open platform for software vendors.
D. The hardware vendor and software vendor should always be different for the sake of security.

Answer: B

Explanation:
With a Type 1 hypervisor, the management software and hardware are tightly tied together and provided by the same vendor on a closed platform. This allows for optimal security, performance, and support. The other answers are all incorrect descriptions of a Type 1 hypervisor.

NEW QUESTION 90
- (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 92
- (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 95
- (Exam Topic 4)
When using an IaaS solution, what is the capability provided to the customer?

A. To provision processing, storage, networks, and other fundamental computing resources when the consumer is able to deploy and run arbitrary software, which

can include OSs and applications.
B. To provision processing, storage, networks, and other fundamental computing resources when the auditor is able to deploy and run arbitrary software, which can include OSs and applications.
C. To provision processing, storage, networks, and other fundamental computing resources when the provider is able to deploy and run arbitrary software, which can include OSs and applications.
D. To provision processing, storage, networks, and other fundamental computing resources when the consumer is not able to deploy and run arbitrary software, which can include OSs and applications.

Answer: A

Explanation:
According to “The NIST Definition of Cloud Computing,” in IaaS, “the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

NEW QUESTION 100
- (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 104
- (Exam Topic 4)
Which of the following is NOT a commonly used communications method within cloud environments to secure data in transit?

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

Answer: D

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

NEW QUESTION 107
- (Exam Topic 4)
Which ITIL component is focused on anticipating predictable problems and ensuring that configurations and operations are in place to prevent these problems from ever occurring?

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

Answer: D

Explanation:
Problem management is focused on identifying and mitigating known problems and deficiencies before they are able to occur, as well as on minimizing the impact of incidents that cannot be prevented. 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. 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 108
- (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 113
- (Exam Topic 4)
A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence.
Which core concept of cloud computing is most related to vendor lock-in?

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

Answer: C

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

NEW QUESTION 114
- (Exam Topic 4)
In a federated identity arrangement using a trusted third-party model, who is the identity provider and who is the relying party?

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

Answer: D

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

NEW QUESTION 118
- (Exam Topic 4)
Just like the risk management process, the BCDR planning process has a defined sequence of steps and processes to follow to ensure the production of a comprehensive and successful plan.
Which of the following is the correct sequence of steps for a BCDR plan?

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

Answer: A

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

NEW QUESTION 122
- (Exam Topic 4)
Which protocol operates at the network layer and provides for full point-to-point encryption of all communications and transmissions?

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

Answer: A

Explanation:
IPSec is a protocol for encrypting and authenticating packets during transmission between two parties and can involve any type of device, application, or service. The protocol performs both the authentication and negotiation of security policies between the two parties at the start of the connection and then maintains these policies throughout the lifetime of the connection. TLS operates at the application layer, not the network layer, and is widely used to secure communications

between two parties. SSL is similar to TLS but has been deprecated. Although a VPN allows a secure channel for communications into a private network from an outside location, it's not a protocol.

NEW QUESTION 123
- (Exam Topic 4)
User access to the cloud environment can be administered in all of the following ways except:

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

Answer: D

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

NEW QUESTION 124
- (Exam Topic 4)
Which protocol, as a part of TLS, handles the actual secure communications and transmission of data?

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

Answer: D

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

NEW QUESTION 127
- (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 131
- (Exam Topic 4)
What is the term we use to describe the general ease and efficiency of moving data from one cloud provider either to another cloud provider or down from the cloud?

A. Obfuscation
B. Elasticity
C. Mobility
D. Portability

Answer: D

Explanation:
Elasticity is the name for the benefit of cloud computing where resources can be apportioned as necessary to meet customer demand. Obfuscation is a technique to hide full raw datasets, either from personnel who do not have need to know or for use in testing. Mobility is not a term pertinent to the CBK.

NEW QUESTION 135
- (Exam Topic 4)
Which of the following is a valid risk management metric?

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

Answer: B

Explanation:

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

NEW QUESTION 139
- (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 142
- (Exam Topic 4)
Your IT steering committee has, at a high level, approved your project to begin using cloud services. However, the committee is concerned with getting locked into a single cloud provider and has flagged the ability to easily move between cloud providers as a top priority. It also wants to save costs by reusing components. Which cross-cutting aspect of cloud computing would be your primary focus as your project plan continues to develop and you begin to evaluate cloud providers?

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

Answer: A

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

NEW QUESTION 143
- (Exam Topic 4)
Being in a cloud environment, cloud customers lose a lot of insight and knowledge as to how their data is stored and their systems are deployed. Which concept from the ISO/IEC cloud standards relates to the necessity of the cloud provider to inform the cloud customer on these issues?

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

Answer: B

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

NEW QUESTION 147
- (Exam Topic 4)
Every security program and process should have which of the following?

A. Severe penalties
B. Multifactor authentication
C. Foundational policy
D. Homomorphic encryption

Answer: C

Explanation:
Policy drives all programs and functions in the organization; the organization should not conduct any operations that don’t have a policy governing them. Penalties may or may not be an element of policy, and severity depends on the topic. Multifactor authentication and homomorphic encryption are red herrings here.

NEW QUESTION 149
- (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 153
- (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)
When using a SaaS solution, what is the capability provided to the customer?

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

Answer: D

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

NEW QUESTION 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 158
- (Exam Topic 3)
Where is a DLP solution generally installed when utilized for monitoring data in transit?

A. Network perimeter
B. Database server

C. Application server
D. Web server

Answer: A

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

NEW QUESTION 163
- (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 168
- (Exam Topic 3)
With finite resources available within a cloud, even the largest cloud providers will at times need to determine which customers will receive additional resources first.
What is the term associated with this determination?

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

Answer: C

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

NEW QUESTION 171
- (Exam Topic 3)
With a cloud service category where the cloud customer is provided a full application framework into which to deploy their code and services, which storage types are MOST likely to be available to them?

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

Answer: A

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

NEW QUESTION 175
- (Exam Topic 3)
Jurisdictions have a broad range of privacy requirements pertaining to the handling of personal data and information.
Which jurisdiction requires all storage and processing of data that pertains to its citizens to be done on hardware that is physically located within its borders?

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

Answer: D

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

NEW QUESTION 176
- (Exam Topic 3)
Where is an XML firewall most commonly and effectively deployed in the environment?

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

Answer: D

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

NEW QUESTION 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 183
- (Exam Topic 3)
Your boss has tasked your team with getting your legacy systems and applications connected with new cloud-based services that management has decided are crucial to customer service and offerings.
Which role would you be assuming under this directive?

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

Answer: C

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

NEW QUESTION 187
- (Exam Topic 3)
With software-defined networking (SDN), which two types of network operations are segregated to allow for granularity and delegation of administrative access and functions?

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

Answer: A

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

NEW QUESTION 189
- (Exam Topic 3)
DNSSEC was designed to add a layer of security to the DNS protocol. Which type of attack was the DNSSEC extension designed to mitigate?

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

Answer: C

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

NEW QUESTION 191
- (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 196
- (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 198
- (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 202
- (Exam Topic 3)
Within an IaaS implementation, which of the following would NOT be a metric used to quantify service charges for the cloud customer?

A. Memory
B. Number of users
C. Storage
D. CPU

Answer: B

Explanation:
Within IaaS, where the cloud customer is responsible for everything beyond the physical network, the number of users on a system would not be a factor in billing or service charges. The core cloud services for IaaS are based on the memory, storage, and CPU requirements of the cloud customer. Because the cloud customer with IaaS is responsible for its own images and deployments, these components comprise the basis of its cloud provisioning and measured services billing.

NEW QUESTION 204
- (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 209
- (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 213
- (Exam Topic 3)
There is a large gap between the privacy laws of the United States and those of the European Union. Bridging this gap is necessary for American companies to do business with European companies and in European markets in many situations, as the American companies are required to comply with the stricter requirements.
Which US program was designed to help companies overcome these differences?

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

Answer: D

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

NEW QUESTION 218
- (Exam Topic 3)
The share phase of the cloud data lifecycle involves allowing data to leave the application, to be shared with external systems, services, or even other vendors/contractors.
What technology would be useful for protecting data at this point?

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

Answer: B

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

NEW QUESTION 222
- (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 227
- (Exam Topic 3)
Where is a DLP solution generally installed when utilized for monitoring data in use?

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

Answer: D

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

NEW QUESTION 230
- (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 233
- (Exam Topic 3)
One of the main components of system audits is the ability to track changes over time and to match these changes with continued compliance and internal processes.
Which aspect of cloud computing makes this particular component more challenging than in a traditional data center?

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

Answer: B

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

NEW QUESTION 235
- (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 240
- (Exam Topic 3)
Humidity levels for a data center are a prime concern for maintaining electrical and computing resources properly as well as ensuring that conditions are optimal for top performance.
Which of the following is the optimal humidity level, as established by ASHRAE?

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

Answer: C

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

NEW QUESTION 241
- (Exam Topic 3)
A crucial decision any company must make is in regard to where it hosts the data systems it depends on. A debate exists as to whether it's best to lease space in a data center or build your own data center--and now with cloud computing, whether to purchase resources within a cloud.
What is the biggest advantage to leasing space in a data center versus procuring cloud services?

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

Answer: B

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

NEW QUESTION 243
- (Exam Topic 3)
Which of the following is NOT one of the main intended goals of a DLP solution?

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

Answer: B

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

NEW QUESTION 244
- (Exam Topic 3)
The management plane is used to administer a cloud environment and perform administrative tasks across a variety of systems, but most specifically it's used with the hypervisors.
What does the management plane typically leverage for this orchestration?

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

Answer: A

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

NEW QUESTION 247
- (Exam Topic 2)
Which aspect of cloud computing makes it very difficult to perform repeat audits over time to track changes and compliance?

A. Virtualization
B. Multitenancy

C. Resource pooling
D. Dynamic optimization

Answer: A

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

NEW QUESTION 250
- (Exam Topic 2)
Which value refers to the amount of data an organization would need to recover in the event of a BCDR situation in order to reach an acceptable level of operations?

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

Answer: C

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

NEW QUESTION 255
- (Exam Topic 2)
Which of the following is a commonly used tool for maintaining system configurations?

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

Answer: C

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

NEW QUESTION 256
- (Exam Topic 2)
Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?

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

Answer: C

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

NEW QUESTION 257
- (Exam Topic 2)
Which of the following is NOT a function performed by the record protocol of TLS?

A. Encryption
B. Acceleration
C. Authentication
D. Compression

Answer: B

Explanation:
The record protocol of TLS performs the authentication and encryption of data packets, and in some cases compression as well. It does not perform any acceleration functions.

NEW QUESTION 258
- (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 260
- (Exam Topic 2)
Which of the following is NOT an application or utility to apply and enforce baselines on a system?

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

Answer: B

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

NEW QUESTION 262
- (Exam Topic 2)
Which of the following service capabilities gives the cloud customer the most control over resources and configurations?

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

Answer: C

Explanation:
The infrastructure service capability gives the cloud customer substantial control in provisioning and configuring resources, including processing, storage, and network resources.

NEW QUESTION 266
- (Exam Topic 2)
Which of the following is the MOST important requirement and guidance for testing during an audit?

A. Stakeholders
B. Shareholders
C. Management
D. Regulations

Answer: D

Explanation:
During any audit, regulations are the most important factor and guidelines for what must be tested. Although the requirements from management, stakeholders, and shareholders are also important, regulations are not negotiable and pose the biggest risk to any organization for compliance failure.

NEW QUESTION 269
- (Exam Topic 2)
At which stage of the BCDR plan creation phase should security be included in discussions?

A. Define scope
B. Analyze
C. Assess risk
D. Gather requirements

Answer: A

Explanation:
Security should be included in discussions from the very first phase when defining the scope. Adding security later is likely to incur additional costs in time and money, or will result in an incomplete or inadequate plan.

NEW QUESTION 272
- (Exam Topic 2)
Which of the following can be useful for protecting cloud customers from a denial-of-service (DoS) attack against another customer hosted in the same cloud?

A. Reservations
B. Measured service
C. Limits
D. Shares

Answer: A

Explanation:
Reservations ensure that a minimum level of resources will always be available to a cloud customer for them to start and operate their services. In the event of a

DoS attack against one customer, they can guarantee that the other customers will still be able to operate.

NEW QUESTION 276
- (Exam Topic 2)
The SOC Type 2 reports are divided into five principles.
Which of the five principles must also be included when auditing any of the other four principles?

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

Answer: C

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

NEW QUESTION 277
- (Exam Topic 2)
Which entity requires all collection and storing of data on their citizens to be done on hardware that resides within their borders?

A. Russia
B. France
C. Germany
D. United States

Answer: A

Explanation:
Signed into law and effective starting on September 1, 2015, Russian Law 526-FZ establishes that any collecting, storing, or processing of personal information or data on Russian citizens must be done from systems and databases that are physically located with the Russian Federation.

NEW QUESTION 281
- (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 283
- (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 287
- (Exam Topic 2)
What must SOAP rely on for security?

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

Answer: A

Explanation:
Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for passing data, and it must rely on the encryption of those data packages for security.

NEW QUESTION 291
- (Exam Topic 2)
Which of the following service capabilities gives the cloud customer an established and maintained framework to deploy code and applications?

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

Answer: C

Explanation:
The platform service capability provides programming languages and libraries from the cloud provider, where the customer can deploy their own code and applications into a managed and controlled framework.

NEW QUESTION 293
- (Exam Topic 2)
Which of the following would NOT be a reason to activate a BCDR strategy?

A. Staffing loss
B. Terrorism attack
C. Utility disruptions
D. Natural disaster

Answer: A

Explanation:
The loss of staffing would not be a reason to declare a BCDR situation because it does not impact production operations or equipment, and the same staff would be needed for a BCDR situation.

NEW QUESTION 297
- (Exam Topic 2)
Which if the following is NOT one of the three components of a federated identity system transaction?

A. Relying party
B. Identity provider
C. User
D. Proxy relay

Answer: D

NEW QUESTION 302
- (Exam Topic 2)
Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?

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

Answer: A

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

NEW QUESTION 307
- (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 310
- (Exam Topic 2)
Which of the following service capabilities gives the cloud customer the least amount of control over configurations and deployments?

A. Platform

B. Infrastructure
C. Software
D. Desktop

Answer: C

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

NEW QUESTION 315
- (Exam Topic 2)
Which type of testing uses the same strategies and toolsets that hackers would use?

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

Answer: A

Explanation:
Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discovery potential vulnerabilities.

NEW QUESTION 316
- (Exam Topic 1)
Which of the following publishes the most commonly used standard for data center design in regard to tiers and topologies?

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

Answer: B

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

NEW QUESTION 320
- (Exam Topic 1)
Which of the following roles is responsible for creating cloud components and the testing and validation of services?

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

Answer: D

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

NEW QUESTION 325
- (Exam Topic 1)
Which of the following would NOT be considered part of resource pooling with an Infrastructure as a Service implementation?

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

Answer: B

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

NEW QUESTION 326
- (Exam Topic 1)
Which publication from the United States National Institute of Standards and Technology pertains to defining cloud concepts and definitions for the various core components of cloud computing?

A. SP 800-153
B. SP 800-145
C. SP 800-53
D. SP 800-40

Answer: B

Explanation:
NIST Special Publications 800-145 is titled "The NIST Definition of Cloud Computing" and contains definitions and explanations of core cloud concepts and components.

NEW QUESTION 330
- (Exam Topic 1)
What are the two protocols that TLS uses?

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

Answer: A

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

NEW QUESTION 332
- (Exam Topic 1)
When is a virtual machine susceptible to attacks while a physical server in the same state would not be?

A. When it is behind a WAF
B. When it is behind an IPS
C. When it is not patched
D. When it is powered off

Answer: D

Explanation:
A virtual machine is ultimately an image file residing a file system. Because of this, even when a virtual machine is "powered off," it is still susceptible to attacks and modification. A physical server that is powered off would not be susceptible to attacks.

NEW QUESTION 333
- (Exam Topic 1)
What is the first stage of the cloud data lifecycle where security controls can be implemented?

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

Answer: B

Explanation:
The "store" phase of the cloud data lifecycle, which typically occurs simultaneously with the "create" phase, or immediately thereafter, is the first phase where security controls can be implemented. In most case, the manner in which the data is stored will be based on its classification.

NEW QUESTION 335
- (Exam Topic 1)
Which of the following is NOT a criterion for data within the scope of eDiscovery?

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

Answer: D

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

NEW QUESTION 337
- (Exam Topic 1)
Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?

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

Answer: B

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

cost.

NEW QUESTION 339
- (Exam Topic 1)
Within an Infrastructure as a Service model, which of the following would NOT be a measured service?

A. CPU
B. Storage
C. Number of users
D. Memory

Answer: C

Explanation:
Within IaaS, the number of users on a system is not relevant to the particular hosting model in regard to cloud resources. IaaS is focused on infrastructure needs of a system or application. Therefore, a factor such as the number of users that could affect licensing requirements, for example, would apply to the SaaS model, or in some instances to PaaS.

NEW QUESTION 342
- (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 343
- (Exam Topic 1)
Which United States law is focused on PII as it relates to the financial industry?

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

Answer: D

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

NEW QUESTION 344
- (Exam Topic 1)
If you're using iSCSI in a cloud environment, what must come from an external protocol or application?

A. Kerberos support
B. CHAP support
C. Authentication
D. Encryption

Answer: D

Explanation:
iSCSI does not natively support encryption, so another technology such as IPsec must be used to encrypt communications.

NEW QUESTION 346
- (Exam Topic 1)
What is the biggest benefit to leasing space in a data center versus building or maintain your own?

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

Answer: B

Explanation:
When leasing space in a data center, an organization can avoid the enormous startup and building costs associated with a data center, and can instead leverage

economies of scale by grouping with other organizations and sharing costs.

NEW QUESTION 350
- (Exam Topic 1)
Which term relates to the application of scientific methods and practices to evidence?

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

Answer: A

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

NEW QUESTION 354
- (Exam Topic 1)
Which of the following represents a control on the maximum amount of resources that a single customer, virtual machine, or application can consume within a cloud environment?

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

Answer: D

Explanation:
Limits are put in place to enforce a maximum on the amount of memory or processing a cloud customer can use. This can be done either on a virtual machine or as a comprehensive whole for a customer, and is meant to ensure that enormous cloud resources cannot be allocated or consumed by a single host or customer to the detriment of other hosts and customers.

NEW QUESTION 355
- (Exam Topic 1)
What expectation of data custodians is made much more challenging by a cloud implementation, especially with PaaS or SaaS?

A. Data classification
B. Knowledge of systems
C. Access to data
D. Encryption requirements

Answer: B

Explanation:
Under the Federal Rules of Civil Procedure, data custodians are assumed and expected to have full and comprehensive knowledge of the internal design and architecture of their systems. In a cloud environment, especially with PaaS and SaaS, it is impossible for the data custodian to have this knowledge because those systems are controlled by the cloud provider and protected as proprietary knowledge.

NEW QUESTION 356
- (Exam Topic 1)
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 361
- (Exam Topic 1)
Which technology is NOT commonly used for security with data in transit?

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

Answer: A

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

NEW QUESTION 363
- (Exam Topic 1)
Which aspect of cloud computing will be most negatively impacted by vendor lock-in?

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

Answer: D

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

NEW QUESTION 364
- (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 365
- (Exam Topic 1)
What is the only data format permitted with the SOAP API?

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

Answer: D

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

NEW QUESTION 366
- (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 369
- (Exam Topic 1)
GAAPs are created and maintained by which organization?

A. ISO/IEC
B. AICPA
C. PCI Council
D. ISO

Answer: B

Explanation:
The AICPA is the organization responsible for generating and maintaining what are the Generally Accepted Accounting Practices in the United States.

NEW QUESTION 373
- (Exam Topic 1)

What is the best approach for dealing with services or utilities that are installed on a system but not needed to perform their desired function?

A. Remove
B. Monitor
C. Disable
D. Stop

Answer: A

Explanation:
The best practice is to totally remove any unneeded services and utilities on a system to prevent any chance of compromise or use. If they are just disabled, it is possible for them to be inadvertently started again at any point, or another exploit could be used to start them again. Removing also negates the need to patch and maintain them going forward.

NEW QUESTION 376
- (Exam Topic 1)
Which of the following are the storage types associated with IaaS?

A. Volume and object
B. Volume and label
C. Volume and container
D. Object and target

Answer: A

NEW QUESTION 381
- (Exam Topic 1)
Which of the following threat types involves an application developer leaving references to internal information and configurations in code that is exposed to the client?

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

Answer: C

Explanation:
An insecure direct object reference occurs when a developer has in their code a reference to something on the application side, such as a database key, the directory structure of the application, configuration information about the hosting system, or any other information that pertains to the workings of the application that should not be exposed to users or the network. 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, allowing spoofing for malware of phishing attacks. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data. Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner.

NEW QUESTION 382
- (Exam Topic 1)
Which of the following threat types involves the sending of untrusted data to a user's browser to be executed with their own credentials and access?

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

Answer: B

Explanation:
Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or where the code is not properly
escaped from processing by the browser. The code is then executed on the user's browser with the user's own access and permissions, allowing an attacker to redirect their web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access.

NEW QUESTION 386
- (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 390

......