Exam Questions CCSP

Certified Cloud Security Professional

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

NEW QUESTION 1
- (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 2
- (Exam Topic 4)
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the required amount of time to restore services to the predetermined level?

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

Answer: C

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

NEW QUESTION 3
- (Exam Topic 4)
Which of the following areas of responsibility always falls completely under the purview of the cloud provider, regardless of which cloud service category is used?

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

Answer: C

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

NEW QUESTION 4
- (Exam Topic 4)
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 5
- (Exam Topic 4)
When data discovery is undertaken, three main approaches or strategies are commonly used to determine what the type of data, its format, and composition are for the purposes of classification.
Which of the following is NOT one of the three main approaches to data discovery?

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

Answer: B

Explanation:
Hashing involves taking a block of data and, through the use of a one-way operation, producing a fixed-size value that can be used for comparison with other data. It is used primarily for protecting data and allowing for rapid comparison when matching data values such as passwords. Labels involve looking for header information or other categorizations of data to determine its type and possible classifications. Metadata involves looking at information attributes of the data, such as creator, application, type, and so on, in determining classification. Content analysis involves examining the actual data itself for its composition and classification level.

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

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

Answer: A

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

NEW QUESTION 8
- (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 9
- (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 10
- (Exam Topic 4)
Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?

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

Answer: B

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

NEW QUESTION 10
- (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 15
- (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 16
- (Exam Topic 4)
Which of the following is not a way to manage risk?

A. Transferring
B. Accepting
C. Mitigating
D. Enveloping

Answer: D

Explanation:
Enveloping is a nonsense term, unrelated to risk management. The rest are not.

NEW QUESTION 18
- (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 19
- (Exam Topic 4)
What are the U.S. State Department controls on technology exports known as?

A. DRM

B. ITAR
C. EAR
D. EAL

Answer: B

Explanation:
ITAR is a Department of State program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Digital rights management tools are used for protecting electronic processing of intellectual property.

NEW QUESTION 23
- (Exam Topic 4)
A variety of security systems can be integrated within a network--some that just monitor for threats and issue alerts, and others that take action based on signatures, behavior, and other types of rules to actively stop potential threats.
Which of the following types of technologies is best described here?

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

Answer: B

Explanation:
An intrusion prevention system (IPS) can inspect traffic and detect any suspicious traffic based on a variety of factors, but it can also actively block such traffic. Although an IDS can detect the same types of suspicious traffic as an IPS, it is only design to alert, not to block. A firewall is only concerned with IP addresses, ports, and protocols; it cannot be used for the signature-based detection of traffic. A proxy can limit or direct traffic based on more extensive factors than a network firewall can, but it's not capable of using the same signature detection rules as an IPS.

NEW QUESTION 27
- (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 30
- (Exam Topic 4)
Which kind of SSAE audit report is most beneficial for a cloud customer, even though it's unlikely the cloud provider will share it?

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

Answer: C

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

NEW QUESTION 32
- (Exam Topic 4)
Cryptographic keys for encrypted data stored in the cloud should be _____.

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

Answer: A

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

NEW QUESTION 33
- (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 38
- (Exam Topic 4)
Which of the following is NOT a component of access control?

A. Accounting
B. Federation
C. Authorization
D. Authentication

Answer: B

Explanation:
Federation is not a component of access control. Instead, it is used to allow users possessing credentials from other authorities and systems to access services outside of their domain. This allows for access and trust without the need to create additional, local credentials. Access control encompasses not only the key concepts of authorization and authentication, but also accounting. Accounting consists of collecting and maintaining logs for both authentication and authorization for operational and regulatory requirements.

NEW QUESTION 42
- (Exam Topic 4)
What type of solution is at the core of virtually all directory services?

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

Answer: B

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

NEW QUESTION 43
- (Exam Topic 4)
Which of the following best describes SAML?

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

Answer: D

NEW QUESTION 45
- (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 46
- (Exam Topic 4)
Which data protection strategy would be useful for a situation where the ability to remove sensitive data from a set is needed, but a requirement to retain the ability to map back to the original values is also present?

A. Masking
B. Tokenization
C. Encryption

D. Anonymization

Answer: B

Explanation:
Tokenization involves the replacement of sensitive data fields with key or token values, which can ultimately be mapped back to the original, sensitive data values. Masking refers to the overall approach to covering
sensitive data, and anonymization is a type of masking, where indirect identifiers are removed from a data set to prevent the mapping back of data to an individual. Encryption refers to the overall process of protecting data via key pairs and protecting confidentiality.

NEW QUESTION 51
- (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 55
- (Exam Topic 4)
Which of the following best describes data masking?

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

Answer: A

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

NEW QUESTION 59
- (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 60
- (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 63
- (Exam Topic 4)
An audit scope statement defines the limits and outcomes from an audit.
Which of the following would NOT be included as part of an audit scope statement?

A. Reports
B. Certification
C. Billing
D. Exclusions

Answer: C

Explanation:
Billing for an audit, or other cost-related items, would not be part of an audit scope statement and would instead be handled prior to the actual audit as part of the contract between the organization and auditors. Reports, exclusions to the scope of the audit, and required certifications on behalf of the systems or auditors are all crucial elements of an audit scope statement.

NEW QUESTION 64
- (Exam Topic 4)
Which of the following is a management role, versus a technical role, as it pertains to data management and oversight?

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

Answer: A

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

NEW QUESTION 65
- (Exam Topic 4)
Which of the following are attributes of cloud computing?

A. Minimal management effort and shared resources
B. High cost and unique resources
C. Rapid provisioning and slow release of resources
D. Limited access and service provider interaction

Answer: A

Explanation:
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NEW QUESTION 68
- (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 73
- (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 75

- (Exam Topic 4)
What is one of the reasons a baseline might be changed?

A. Numerous change requests
B. To reduce redundancy
C. Natural disaster
D. Power fluctuation

Answer: A

Explanation:
If the CMB is receiving numerous change requests to the point where the amount of requests would drop by modifying the baseline, then that is a good reason to change the baseline. None of the other reasons should involve the baseline at all.

NEW QUESTION 77
- (Exam Topic 4)
Which of the following is NOT a major regulatory framework?

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

Answer: D

Explanation:
FIPS 140-2 is a United States certification standard for cryptographic modules, and it provides guidance and requirements for their use based on the requirements of the data classification. However, these are not actual regulatory requirements. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS) are all major regulatory frameworks either by law or specific to an industry.

NEW QUESTION 82
- (Exam Topic 4)
What is the correct order of the phases of the data life cycle?

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

Answer: D

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

NEW QUESTION 83
- (Exam Topic 4)
Data masking can be used to provide all of the following functionality, except:

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

Answer: B

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

NEW QUESTION 84
- (Exam Topic 4)
All policies within the organization should include a section that includes all of the following, except:

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

Answer: A

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

NEW QUESTION 86
- (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 88
- (Exam Topic 4)
The GAPP framework was developed through a joint effort between the major Canadian and American
professional accounting associations in order to assist their members with managing and preventing risks to the privacy of their data and customers.
Which of the following is the meaning of GAPP?

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

Answer: C

NEW QUESTION 90
- (Exam Topic 4)
Your new CISO is placing increased importance and focus on regulatory compliance as your applications and systems move into cloud environments.
Which of the following would NOT be a major focus of yours as you develop a project plan to focus on regulatory compliance?

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

Answer: D

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

NEW QUESTION 91
- (Exam Topic 4)
Data labels could include all the following, except:

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

Answer: A

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

NEW QUESTION 95
- (Exam Topic 4)
Which crucial aspect of cloud computing can be most threatened by insecure APIs?

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

Answer: A

Explanation:
Cloud environments depend heavily on API calls for management and automation. Any vulnerability with the APIs can cause significant risk and exposure to all tenants of the cloud environment. Resource pooling and elasticity could both be impacted by insecure APIs, as both require automation and orchestration to operate properly, but automation is the better answer here. Redundancy would not be directly impacted by insecure APIs.

NEW QUESTION 96
- (Exam Topic 4)
A localized incident or disaster can be addressed in a cost-effective manner by using which of the following?

A. UPS

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

Answer: C

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

NEW QUESTION 98
- (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 100
- (Exam Topic 4)
The baseline should cover which of the following?

A. Data breach alerting and reporting
B. All regulatory compliance requirements
C. As many systems throughout the organization as possible
D. A process for version control

Answer: C

Explanation:
The more systems that be included in the baseline, the more cost-effective and scalable the baseline is. The baseline does not deal with breaches or version control; those are the provinces of the security office and CMB, respectively. Regulatory compliance might (and usually will) go beyond the baseline and involve systems, processes, and personnel that are not subject to the baseline.

NEW QUESTION 101
- (Exam Topic 4)
For performance purposes, OS monitoring should include all of the following except:

A. Disk space
B. Disk I/O usage
C. CPU usage
D. Print spooling

Answer: D

Explanation:
Print spooling is not a metric for system performance; all the rest are.

NEW QUESTION 104
- (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 105
- (Exam Topic 4)
The goals of DLP solution implementation include all of the following, except:

A. Elasticity
B. Policy enforcement
C. Data discovery
D. Loss of mitigation

Answer: A

Explanation:
DLP does not have anything to do with elasticity, which is the capability of the environment to scale up or down according to demand. All the rest are goals of DLP implementations.

NEW QUESTION 109
- (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 113
- (Exam Topic 4)
Which of the following methods of addressing risk is most associated with insurance?

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

Answer: B

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

NEW QUESTION 115
- (Exam Topic 4)
What concept does the A represent within the DREAD model?

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

Answer: A

Explanation:
The concept of affected users measures the percentage of users who would be impacted by a successful exploit. Scoring ranges from 0, which would impact no users, to 10, which would impact all users. None of the other options provided is the correct term.

NEW QUESTION 120
- (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 123
- (Exam Topic 4)
When a system needs to be exposed to the public Internet, what type of secure system would be used to perform only the desired operations?

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

Answer: D

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

NEW QUESTION 128
- (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 129
- (Exam Topic 4)
Many activities within a cloud environment are performed via programmatic means, where complex and distributed operations are handled without the need to perform each step individually.
Which of the following concepts does this describe?

A. Orchestration
B. Provisioning
C. Automation
D. Allocation

Answer: A

Explanation:
Orchestration is the programmatic means of managing and coordinating activities within a cloud environment and allowing for a commensurate level of automation and self-service. Provisioning, allocation, and automation are all components of orchestration, but none refers to the overall concept.

NEW QUESTION 133
- (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 134
- (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 135
- (Exam Topic 4)
What concept and operational process must be spelled out clearly, as far as roles and responsibilities go, between the cloud provider and cloud customer for the mitigation of any problems or security events?

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

Answer: A

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

NEW QUESTION 137
- (Exam Topic 4)
Which of the following is NOT one of the components of multifactor authentication?

A. Something the user knows
B. Something the user has
C. Something the user sends
D. Something the user is

Answer: C

Explanation:
Multifactor authentication systems are composed of something the user knows, has, and/or is, not something the user sends. Multifactor authentication commonly uses something that a user knows, has, and/or is (such as biometrics or features).

NEW QUESTION 141
- (Exam Topic 4)
Which of the following are considered to be the building blocks of cloud computing?

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

Answer: A

NEW QUESTION 143
- (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 145
- (Exam Topic 4)
When reviewing the BIA after a cloud migration, the organization should take into account new factors related to data breach impacts. One of these new factors is:

A. Many states have data breach notification laws.
B. Breaches can cause the loss of proprietary data.
C. Breaches can cause the loss of intellectual property.
D. Legal liability can't be transferred to the cloud provider.

Answer: D

Explanation:
State notification laws and the loss of proprietary data/intellectual property pre-existed the cloud; only the lack of ability to transfer liability is new.

NEW QUESTION 150
- (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 155
- (Exam Topic 4)
Upon completing a risk analysis, a company has four different approaches to addressing risk. Which approach it takes will be based on costs, available options, and adherence to any regulatory requirements from independent audits.
Which of the following groupings correctly represents the four possible approaches?

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

Answer: A

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

NEW QUESTION 158
- (Exam Topic 4)
DLP can be combined with what other security technology to enhance data controls?

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

Answer: C

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

NEW QUESTION 163
- (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 166
- (Exam Topic 4)
To protect data on user devices in a BYOD environment, the organization should consider requiring all the following, except:

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

Answer: C

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

NEW QUESTION 169
- (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 170
- (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 173
- (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 174
- (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 176
- (Exam Topic 4)
Maintenance mode requires all of these actions except:

A. Remove all active production instances
B. Ensure logging continues
C. Initiate enhanced security controls
D. Prevent new logins

Answer: C

Explanation:
While the other answers are all steps in moving from normal operations to maintenance mode, we do not necessarily initiate any enhanced security controls.

NEW QUESTION 177
- (Exam Topic 4)
The various models generally available for cloud BC/DR activities include all of the following except:

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

Answer: D

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

NEW QUESTION 181
- (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 183
- (Exam Topic 4)
When an organization is considering the use of cloud services for BCDR planning and solutions, which of the following cloud concepts would be the most important?

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

Answer: D

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

NEW QUESTION 185
- (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 190
- (Exam Topic 4)
In the cloud motif, the data owner is usually:

A. The cloud provider
B. In another jurisdiction
C. The cloud customer
D. The cloud access security broker

Answer: C

Explanation:
The data owner is usually considered the cloud customer in a cloud configuration; the data in question is the customer's information, being processed in the cloud. The cloud provider is only leasing services and hardware to the customer. The cloud access security broker (CASB) only handles access control on behalf of the cloud customer, and is not in direct contact with the production data.

NEW QUESTION 193
- (Exam Topic 4)
Which of the following is not an example of a highly regulated environment?

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

Answer: D

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

NEW QUESTION 196
- (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 201
- (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 206
- (Exam Topic 4)
In the cloud motif, the data processor is usually:

A. The cloud customer

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

Answer: B

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

NEW QUESTION 209
- (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 212
- (Exam Topic 4)
SOC Type 1 reports are considered "restricted use," in that they are intended only for limited audiences and purposes.
Which of the following is NOT a population that would be appropriate for a SOC Type 1 report?

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

Answer: C

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

NEW QUESTION 216
- (Exam Topic 4)
What is the concept of isolating an application from the underlying operating system for testing purposes?

A. Abstracting
B. Application virtualization
C. Hosting
D. Sandboxing

Answer: B

Explanation:
Application virtualization is a software implementation that allows applications and programs to run in an isolated environment rather than directly interacting with the operating system. Sandboxing refers to segregating information or processes for security or testing purposes, but it's not directly related to isolation from the underlying operating system. Abstracting sounds similar to the correct term but is not pertinent to the question, and hosting is provided as an erroneous answer.

NEW QUESTION 217
- (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 219
- (Exam Topic 4)
Which aspect of cloud computing serves as the biggest challenge to using DLP to protect data at rest?

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

Answer: B

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

NEW QUESTION 220
- (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 221
- (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 226
- (Exam Topic 4)
Which is the lowest level of the CSA STAR program?

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

Answer: B

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

NEW QUESTION 230
- (Exam Topic 4)
In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?

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

Answer: B

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

for ensuring compliance with regulations. HIPAA is a statute.

NEW QUESTION 235
- (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 238
- (Exam Topic 4)
Your company is in the planning stages of moving applications that have large data sets to a cloud environment.
What strategy for data removal would be the MOST appropriate for you to recommend if costs and speed are primary considerations?

A. Shredding
B. Media destruction
C. Crypthographic erasure
D. Overwriting

Answer: C

Explanation:
Cryptographic erasure involves having the data encrypted, typically as a matter of standard operations, and then rendering the data useless and unreadable by destroying the encryption keys for it. It represents a very cheap and immediate way to destroy data, and it works in all environments. With a cloud environment and multitenancy, media destruction or the physical destruction of storage devices, including shredding, would not be possible. Depending on the environment, overwriting may or may not be possible, but cryptographic erasure is the best answer because it is always an available option and is very quick to implement.

NEW QUESTION 239
- (Exam Topic 4)
Which of the following is NOT one of the official risk rating categories?

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

Answer: C

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

NEW QUESTION 242
- (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 247
- (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 251
- (Exam Topic 3)
A DLP solution/implementation has three main components. Which of the following is NOT one of the three main components?

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

Answer: C

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

NEW QUESTION 255
- (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 256
- (Exam Topic 3)
What does a cloud customer purchase or obtain from a cloud provider?

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

Answer: A

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

NEW QUESTION 257
- (Exam Topic 3)
During which phase of the cloud data lifecycle is it possible for the classification of data to change?

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

Answer: C

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

NEW QUESTION 260
- (Exam Topic 3)
Which cloud deployment model would be ideal for a group of universities looking to work together, where each university can gain benefits according to its specific needs?

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

Answer: D

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

NEW QUESTION 263
- (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 265
- (Exam Topic 3)
Which data state would be most likely to use digital signatures as a security protection mechanism?

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

Answer: A

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

NEW QUESTION 266
- (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 270
- (Exam Topic 3)
Within a federated identity system, which entity accepts tokens from the identity provider?

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

Answer: D

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

NEW QUESTION 272
- (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 274
- (Exam Topic 3)
Audits are either done based on the status of a system or application at a specific time or done as a study over a period of time that takes into account changes and processes.
Which of the following pairs matches an audit type that is done over time, along with the minimum span of time necessary for it?

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

Answer: D

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

NEW QUESTION 277
- (Exam Topic 3)
Which of the following threat types involves an application that does not validate authorization for portions of itself beyond when the user first enters it?

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

Answer: B

Explanation:
It is imperative that applications do checks when each function or portion of the application is accessed to ensure that the user is properly authorized. Without continual checks each time a function is accessed, an attacker could forge requests to access portions of the application where authorization has not been granted. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.

NEW QUESTION 278
- (Exam Topic 3)
In the wake of many scandals with major corporations involving fraud and the deception of investors and regulators, which of the following laws was passed to govern accounting and financial records and disclosures?

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

Answer: D

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

NEW QUESTION 281
- (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 284
- (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 289
- (Exam Topic 3)
From a security perspective, what component of a cloud computing infrastructure represents the biggest concern?

A. Hypervisor
B. Management plane
C. Object storage
D. Encryption

Answer: B

Explanation:
The management plane will have broad administrative access to all host systems throughout an environment; as such, it represents the most pressing security concerns. A compromise of the management plane can directly lead to compromises of any other systems within the environment. Although hypervisors represent a significant security concern to an environment because their compromise would expose any virtual systems hosted within them, the management plane is a better choice in this case because it controls multiple hypervisors. Encryption and object storage both represent lower-level security concerns.

NEW QUESTION 293
- (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 297
- (Exam Topic 3)
Which of the following is not a risk management framework?

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

Answer: B

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

NEW QUESTION 298
- (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 302
- (Exam Topic 3)
Which of the following threat types involves the sending of commands or arbitrary data through input fields in an application in an attempt to get that code executed as part of normal processing?

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

Answer: C

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

NEW QUESTION 306
- (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 311
- (Exam Topic 3)
With IaaS, what is responsible for handling the security and control over the volume storage space?

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

Answer: B

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

NEW QUESTION 314
- (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 315
- (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 320
- (Exam Topic 3)
In order to comply with regulatory requirements, which of the following secure erasure methods would be available to a cloud customer using volume storage within the IaaS service model?

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

Answer: D

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

NEW QUESTION 322
- (Exam Topic 3)
Three central concepts define what type of data and information an organization is responsible for pertaining to eDiscovery.
Which of the following are the three components that comprise required disclosure?

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

Answer: D

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

NEW QUESTION 323
- (Exam Topic 3)
With a cloud service category where the cloud customer is responsible for deploying all services, systems, and components needed for their applications, which of the following storage types are MOST likely to be available to them?

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

Answer:

B

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

NEW QUESTION 325
- (Exam Topic 3)
When dealing with PII, which category pertains to those requirements that can carry legal sanctions or penalties for failure to adequately safeguard the data and address compliance requirements?

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

Answer: C

Explanation:
Regulated PII pertains to data that is outlined in law and regulations. Violations of the requirements for the protection of regulated PII can carry legal sanctions or penalties. Contractual PII involves required data protection that is determined by the actual service contract between the cloud provider and cloud customer, rather than outlined by law. Violations of the provisions of contractual PII carry potential financial or contractual implications, but not legal sanctions. Legal and jurisdictional are similar terms to regulated, but neither is the official term used.

NEW QUESTION 327
- (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 328
- (Exam Topic 3)
Digital investigations have adopted many of the same methodologies and protocols as other types of criminal or scientific inquiries.
What term pertains to the application of scientific norms and protocols to digital investigations?

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

Answer: D

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

NEW QUESTION 330
- (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 333
- (Exam Topic 3)

Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.
Which of the following is NOT a regulatory system from the United States federal government?

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

Answer: D

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

NEW QUESTION 337
- (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 341
- (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 345
- (Exam Topic 3)
Which of the following tasks within a SaaS environment would NOT be something the cloud customer would be responsible for?

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

Answer: A

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

NEW QUESTION 348
- (Exam Topic 3)
Configurations and policies for a system can come from a variety of sources and take a variety of formats. Which concept pertains to the application of a set of configurations and policies that is applied to all systems or a class of systems?

A. Hardening
B. Leveling
C. Baselines

D. Standards

Answer: C

Explanation:
Baselines are a set of configurations and policies applied to all new systems or services, and they serve as the basis for deploying any other services on top of them. Although standards often form the basis for baselines, the term is applicable in this case. Hardening is the process of securing a system, often through the application of baselines. Leveling is an extraneous but similar term to baselining.

NEW QUESTION 350
- (Exam Topic 3)
If you are running an application that has strict legal requirements that the data cannot reside on systems that contain other applications or systems, which aspect of cloud computing would be prohibitive in this case?

A. Multitenancy
B. Broad network access
C. Portability
D. Elasticity

Answer: A

Explanation:
Multitenancy is the aspect of cloud computing that involves having multiple customers and applications running within the same system and sharing the same resources. Although considerable mechanisms are in place to ensure isolation and separation, the data and applications are ultimately using shared resources. Broad network access refers to the ability to access cloud services from any location or client. Portability refers to the ability to easily move cloud services between different cloud providers, whereas elasticity refers to the capabilities of a cloud environment to add or remove services, as needed, to meet current demand.

NEW QUESTION 353
- (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 356
- (Exam Topic 3)
Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?

A. Regulation
B. Multitenancy
C. Virtualization
D. Resource pooling

Answer: B

Explanation:
With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers. Especially within a public cloud model, it is not possible or practical for a cloud provider to alter its services for specific customer demands. Resource pooling and virtualization within a cloud environment would be the same for all customers, and would not impact certifications that a cloud provider might be willing to pursue. Regulations would form the basis for certification problems and would be a reason for a cloud provider to pursue specific certifications to meet customer requirements.

NEW QUESTION 361
- (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 363
- (Exam Topic 2)

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

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

Answer: C

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

NEW QUESTION 368
- (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 373
- (Exam Topic 2)
What concept does the "I" represent with the STRIDE threat model?

A. Integrity
B. Information disclosure
C. IT security
D. Insider threat

Answer: B

Explanation:
Perhaps the biggest concern for any user is having their personal and sensitive information disclosed by an application. There are many aspects of an application to consider with security and protecting this information, and it is very difficult for any application to fully ensure security from start to finish. The obvious focus is on security within the application itself, as well as protecting and storing the data.

NEW QUESTION 376
- (Exam Topic 2)
Which of the following is NOT a key area for performance monitoring as far as an SLA is concerned?

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

Answer: B

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

NEW QUESTION 380
- (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 382
- (Exam Topic 2)
Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?

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

Answer: D

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

NEW QUESTION 383
- (Exam Topic 2)
What does dynamic application security testing (DAST) NOT entail?

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

Answer: D

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

NEW QUESTION 385
- (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 386
- (Exam Topic 2)
What is the biggest challenge to data discovery in a cloud environment?

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

Answer: C

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

NEW QUESTION 391
- (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 393
- (Exam Topic 2)
Where is an XML firewall most commonly deployed in the environment?

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

Answer: D

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

NEW QUESTION 397
- (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 398
- (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 400
- (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 403
- (Exam Topic 2)
Which value refers to the percentage of production level restoration needed to meet BCDR objectives?

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

Answer: C

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

NEW QUESTION 408
- (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 410
- (Exam Topic 2)
What is a standard configuration and policy set that is applied to systems and virtual machines called?

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

Answer: B

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

NEW QUESTION 412
- (Exam Topic 2)
Other than cost savings realized due to measured service, what is another facet of cloud computing that will typically save substantial costs in time and money for an organization in the event of a disaster?

A. Broad network access
B. Interoperability
C. Resource pooling
D. Portability

Answer: A

Explanation:
With a typical BCDR solution, an organization would need some number of staff to quickly travel to the location of the BCDR site to configure systems and applications for recovery. With a cloud environment, everything is done over broad network access, with no need (or even possibility) to travel to a remote site at any time.

NEW QUESTION 417
- (Exam Topic 2)
Which European Union directive pertains to personal data privacy and an individual's control over their personal data?

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

Answer: B

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

NEW QUESTION 418
- (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 419
- (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 422
- (Exam Topic 2)
What type of security threat is DNSSEC designed to prevent?

A. Account hijacking
B. Snooping
C. Spoofing
D. Injection

Answer: C

Explanation:
DNSSEC is designed to prevent the spoofing and redirection of DNS resolutions to rogue sites.

NEW QUESTION 425
- (Exam Topic 2)
What process is used within a clustered system to provide high availability and load balancing?

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

Answer: D

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

NEW QUESTION 430
- (Exam Topic 2)
What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?

A. Proxy
B. Bastion
C. Honeypot
D. WAF

Answer: B

Explanation:
A bastion host is a server that is fully exposed to the public Internet, but is extremely hardened to prevent attacks and is usually dedicated for a specific application or usage; it is not something that will serve multiple purposes. This singular focus allows for much more stringent security hardening and monitoring.

NEW QUESTION 432
- (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 436
- (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 440

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

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

Answer: D

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

NEW QUESTION 443
- (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 444
- (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 445
- (Exam Topic 2)
Who would be responsible for implementing IPsec to secure communications for an application?

A. Developers
B. Systems staff
C. Auditors
D. Cloud customer

Answer: B

Explanation:
Because IPsec is implemented at the system or network level, it is the responsibility of the systems staff. IPsec removes the responsibility from developers, whereas other technologies such as TLS would be implemented by developers.

NEW QUESTION 447
- (Exam Topic 2)
Which of the following is a restriction that can be enforced by information rights management (IRM) that is not possible for traditional file system controls?

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

Answer: D

Explanation:
IRM allows an organization to control who can print a set of information. This is not be possible under traditional file system controls, where if a user can read a file, they are able to print it as well.

NEW QUESTION 449
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the ability for a cloud customer to easily remove their applications and data from a cloud environment?

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

Answer: A

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

NEW QUESTION 450
- (Exam Topic 2)
Which of the following is NOT a focus or consideration of an internal audit?

A. Certification
B. Design
C. Costs
D. Operational efficiency

Answer: A

Explanation:
In order to obtain and comply with certifications, independent external audits must be performed and satisfied. Although some testing of certification controls can be part of an internal audit, they will not satisfy requirements.

NEW QUESTION 451
- (Exam Topic 2)
What is the concept of segregating information or processes, within the same system or application, for security reasons?

A. fencing
B. Sandboxing
C. Cellblocking
D. Pooling

Answer: B

Explanation:
Sandboxing involves segregating and isolating information or processes from others within the same system or application, typically for security concerns. This is generally used for data isolation (for example, keeping different communities and populations of users isolated from other similar data).

NEW QUESTION 453
- (Exam Topic 2)
Which aspect of cloud computing makes data classification even more vital than in a traditional data center?

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

Answer: C

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

NEW QUESTION 457
- (Exam Topic 1)
What does SDN stand for within a cloud environment?

A. Software-dynamic networking
B. Software-defined networking
C. Software-dependent networking
D. System-dynamic nodes

Answer: B

Explanation:
Software-defined networking separates the administration of network filtering and network forwarding to allow for distributed administration.

NEW QUESTION 459
- (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 464
- (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 465
- (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 470
- (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 475
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CCSP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CCSP Product From:

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

Money Back Guarantee

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