Exam Questions CCSP

Certified Cloud Security Professional

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

NEW QUESTION 1
- (Exam Topic 4)
What is the intellectual property protection for a confidential recipe for muffins?

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

Answer: C

Explanation:
Confidential recipes unique to the organization are trade secrets. The other answers listed are answers to other questions.

NEW QUESTION 2
- (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 3
- (Exam Topic 4)
Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like:

A. Ransomware
B. Syn floods
C. XSS and SQL injection
D. Password cracking

Answer: C

Explanation:
WAFs detect how the application interacts with the environment, so they are optimal for detecting and refuting things like SQL injection and XSS. Password cracking, syn floods, and ransomware usually aren’t taking place in the same way as injection and XSS, and they are better addressed with controls at the router and through the use of HIDS, NIDS, and antimalware tools.

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

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

Answer: A

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

NEW QUESTION 5
- (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 6
- (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 7
- (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 8
- (Exam Topic 4)
What is the experimental technology that might lead to the possibility of processing encrypted data without having to decrypt it first?

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

Answer: C

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

NEW QUESTION 9
- (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 10
- (Exam Topic 4)
Database activity monitoring (DAM) can be:

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

Answer: A

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

NEW QUESTION 10
- (Exam Topic 4)
Which of the following frameworks focuses specifically on design implementation and management?

A. ISO 31000:2009

B. ISO 27017
C. NIST 800-92
D. HIPAA

Answer: A

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

NEW QUESTION 14
- (Exam Topic 4)
What is the intellectual property protection for a useful manufacturing innovation?

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

Answer: C

Explanation:
Patents protect processes (as well as inventions, new plantlife, and decorative patterns). The other answers listed are answers to other questions.

NEW QUESTION 16
- (Exam Topic 4)
Gap analysis is performed for what reason?

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

Answer: A

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

NEW QUESTION 20
- (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 25
- (Exam Topic 4)
The cloud customer’s trust in the cloud provider can be enhanced by all of the following except:

A. SLAs
B. Shared administration
C. Audits
D. real-time video surveillance

Answer: D

Explanation:
Video surveillance will not provide meaningful information and will not enhance trust. All the others will do it.

NEW QUESTION 30
- (Exam Topic 4)
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 34
- (Exam Topic 4)
Data labels could include all the following, except:

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

Answer: B

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

NEW QUESTION 37
- (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 38
- (Exam Topic 4)
What's a potential problem when object storage versus volume storage is used within IaaS for application use and dependency?

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

Answer: B

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

NEW QUESTION 43
- (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 47
- (Exam Topic 4)
During the course of an audit, which of the following would NOT be an input into the control requirements used as part of a gap analysis.

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

Answer: C

Explanation:

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

NEW QUESTION 51
- (Exam Topic 4)
With an application hosted in a cloud environment, who could be the recipient of an eDiscovery order?

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

Answer: B

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

NEW QUESTION 52
- (Exam Topic 4)
Which of the following report is most aligned with financial control audits?

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

Answer: C

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

NEW QUESTION 55
- (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 58
- (Exam Topic 4)
In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?

A. Physical
B. All of the above
C. technological
D. Administrative

Answer: B

Explanation:
Layered defense calls for a diverse approach to security.

NEW QUESTION 61
- (Exam Topic 4)
Which of the following is NOT considered a type of data loss?

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

Answer: B

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

NEW QUESTION 63
- (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 64
- (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 67
- (Exam Topic 4)
Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:

A. The cloud provider’s utilities
B. The cloud provider’s suppliers
C. The cloud provider’s resellers
D. The cloud provider’s vendors

Answer: C

Explanation:
The cloud provider’s resellers are a marketing and sales mechanism, not an operational dependency that could affect the security of a cloud customer.

NEW QUESTION 71
- (Exam Topic 4)
Key maintenance and security are paramount within a cloud environment due to the widespread use of encryption for both data and transmissions.
Which of the following key-management systems would provide the most robust control over and ownership of the key-management processes for the cloud customer?

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

Answer: A

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

NEW QUESTION 75
- (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 80
- (Exam Topic 4)
Gathering business requirements can aid the organization in determining all of this information about organizational assets, except:

A. Full inventory
B. Criticality
C. Value
D. Usefulness

Answer: D

Explanation:
When we gather information about business requirements, we need to do a complete inventory, receive accurate valuation of assets (usually from the owners of those assets), and assess criticality; this collection of information does not tell us, objectively, how useful an asset is, however.

NEW QUESTION 81
- (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 82
- (Exam Topic 4)
Which of the following terms is not associated with cloud forensics?

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

Answer: D

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

NEW QUESTION 83
- (Exam Topic 4)
When using an IaaS solution, what is the capability provided to the customer?

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

Answer: A

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

NEW QUESTION 87
- (Exam Topic 4)
When using an IaaS solution, what is a key benefit provided to the customer?

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

Answer: A

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

NEW QUESTION 88
- (Exam Topic 4)
Best practices for key management include all of the following, except:

A. Ensure multifactor authentication
B. Pass keys out of band
C. Have key recovery processes
D. Maintain key security

Answer: A

Explanation:
We should do all of these except for requiring multifactor authentication, which is pointless in key management.

NEW QUESTION 93
- (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 94
- (Exam Topic 4)
Which aspect of data poses the biggest challenge to using automated tools for data discovery and programmatic data classification?

A. Quantity
B. Language
C. Quality
D. Number of courses

Answer: C

Explanation:
The biggest challenge for properly using any programmatic tools in data discovery is the actual quality of the data, including the data being uniform and well structured, labels being properly applied, and other similar facets. Without data being organized in such a manner, it is extremely difficult for programmatic tools to automatically synthesize and make determinations from it. The overall quantity of data, as well as the number of sources, does not pose an enormous challenge for data discovery programs, other than requiring a longer time to process the data. The language of the data itself should not matter to a program that is designed to process it, as long as the data is well formed and consistent.

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

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

Answer: D

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

NEW QUESTION 98
- (Exam Topic 4)
Which ITIL component is focused on anticipating predictable problems and ensuring that configurations and operations are in place to prevent these problems from ever occurring?

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

Answer: D

Explanation:
Problem management is focused on identifying and mitigating known problems and deficiencies before they are able to occur, as well as on minimizing the impact of incidents that cannot be prevented. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Configuration management tracks and maintains detailed information about all IT components within an organization.

NEW QUESTION 99
- (Exam Topic 4)
Many aspects of cloud computing bring enormous benefits over a traditional data center, but also introduce new challenges unique to cloud computing.
Which of the following aspects of cloud computing makes appropriate data classification of high importance?

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

Answer: A

Explanation:
With multitenancy, where different cloud customers all share the same physical systems and networks, data classification becomes even more important to ensure that the appropriate security controls are applied immediately to prevent any potential leakage or exposure to other customers. Portability refers to the ability to move easily from one cloud provider to another. Interoperability refers to the ability to reuse components and services for different uses. Reversibility refers to the ability of the cloud customer to quickly and completely remove all data and services from a cloud provider and to verify the removal.

NEW QUESTION 103
- (Exam Topic 4)
Which of the following components are part of what a CCSP should review when looking at contracting with a cloud service provider?

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

Answer: D

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

NEW QUESTION 104
- (Exam Topic 4)
A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence.
Which core concept of cloud computing is most related to vendor lock-in?

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

Answer: C

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

NEW QUESTION 108
- (Exam Topic 4)
What process entails taking sensitive data and removing the indirect identifiers from each data object so that the identification of a single entity would not be possible?

A. Tokenization

B. Encryption
C. Anonymization
D. Masking

Answer: C

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

NEW QUESTION 109
- (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 113
- (Exam Topic 4)
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the amount of data and services needed to reach the predetermined level of operations?

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

Answer: B

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

NEW QUESTION 117
- (Exam Topic 4)
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 120
- (Exam Topic 4)
There are many situations when testing a BCDR plan is appropriate or mandated. Which of the following would not be a necessary time to test a BCDR plan?

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

Answer: B

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

complete.

NEW QUESTION 125
- (Exam Topic 4)
To address shared monitoring and testing responsibilities in a cloud configuration, the provider might offer all these to the cloud customer except:

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

Answer: C

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

NEW QUESTION 130
- (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 135
- (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 140
- (Exam Topic 4)
What must SOAP rely on for security since it does not provide security as a built-in capability?

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

Answer: A

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

NEW QUESTION 142
- (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 143
- (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 147
- (Exam Topic 4)
Which of the following terms is NOT a commonly used category of risk acceptance?

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

Answer: D

Explanation:

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

NEW QUESTION 149
- (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 152
- (Exam Topic 4)
Tokenization requires two distinct _____.

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

Answer: C

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

NEW QUESTION 156
- (Exam Topic 3)
Where is a DLP solution generally installed when utilized for monitoring data in transit?

A. Network perimeter
B. Database server
C. Application server
D. Web server

Answer: A

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

NEW QUESTION 159
- (Exam Topic 3)
Modern web service systems are designed for high availability and resiliency. Which concept pertains to the ability to detect problems within a system, environment, or application and programmatically invoke redundant systems or processes for mitigation?

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

Answer: C

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

NEW QUESTION 163
- (Exam Topic 3)
An SLA contains the official requirements for contract performance and satisfaction between the cloud provider and cloud customer. Which of the following would NOT be a component with measurable metrics and requirements as part of an SLA?

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

Answer: B

Explanation:
Dealing with users or user access would not be an appropriate item for inclusion in an SLA specifically. However, user access and user experience would be covered indirectly through other metrics. Memory, CPU, and network resources are all typically included within an SLA for availability and response times when dealing with any incidents.

NEW QUESTION 165
- (Exam Topic 3)
Which of the following threat types can occur when baselines are not appropriately applied or when unauthorized changes are made?

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

Answer: A

Explanation:
Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner. This can be due to a shortcoming in security baselines or configurations, unauthorized changes to system configurations, or a failure to patch and upgrade systems as the vendor releases security patches. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, allowing spoofing for malware or phishing attacks. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data.

NEW QUESTION 170
- (Exam Topic 3)
If a cloud computing customer wishes to guarantee that a minimum level of resources will always be available, which of the following set of services would compromise the reservation?

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

Answer: D

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

NEW QUESTION 171
- (Exam Topic 3)
Which cloud service category would be most ideal for a cloud customer that is developing software to test its applications among multiple hosting providers to determine the best option for its needs?

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

Answer: B

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

NEW QUESTION 172
- (Exam Topic 3)
For service provisioning and support, what is the ideal amount of interaction between a cloud customer and cloud provider?

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

Answer: C

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

NEW QUESTION 174
- (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 176
- (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 177
- (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 182
- (Exam Topic 3)
Which of the following roles would be responsible for managing memberships in federations and the use and integration of federated services?

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

Answer: A

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

NEW QUESTION 187
- (Exam Topic 3)
Which of the following statements best describes a Type 1 hypervisor?

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

Answer: D

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

NEW QUESTION 188
- (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 191
- (Exam Topic 3)
Most APIs will support a variety of different data formats or structures.
However, the SOAP API will only support which one of the following data formats?

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

Answer: A

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

NEW QUESTION 196
4 to 80.6 degrees Fahrenheit (or 18 to 27 degrees Celsius) as the optimal temperature range for data centers. None of these options is the recommendation from ASHRAE.

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 198
- (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 203
- (Exam Topic 3)
Firewalls are used to provide network security throughout an enterprise and to control what information can be accessed--and to a certain extent, through what means.
Which of the following is NOT something that firewalls are concerned with?

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

Answer: B

Explanation:
Firewalls work at the network level and control traffic based on the source, destination, protocol, and ports. Whether or not the traffic is encrypted is not a factor with firewalls and their decisions about routing traffic. Firewalls work primarily with IP addresses, ports, and protocols.

NEW QUESTION 205
- (Exam Topic 3)
What type of storage structure does object storage employ to maintain files?

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

Answer: D

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

NEW QUESTION 208
- (Exam Topic 3)
Which of the following threat types involves the sending of invalid and manipulated requests through a user's client to execute commands on the application under their own credentials?

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

Answer: B

Explanation:
A cross-site request forgery (CSRF) attack forces a client that a user has used to authenticate to an application to send forged requests under the user's own credentials to execute commands and requests that the application thinks are coming from a trusted client and user. Although this type of attack cannot be used to steal data directly because the attacker has no way to see the results of the commands, it does open other ways to compromise an application. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. 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.

NEW QUESTION 209
- (Exam Topic 3)
One of the main components of system audits is the ability to track changes over time and to match these changes with continued compliance and internal processes.
Which aspect of cloud computing makes this particular component more challenging than in a traditional data center?

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

Answer: B

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

NEW QUESTION 213
- (Exam Topic 3)
Different types of audits are intended for different audiences, such as internal, external, regulatory, and so on. Which of the following audits are considered "restricted use" versus being for a more broad audience?

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

Answer: B

Explanation:
SOC Type 1 reports are intended for restricted use, only to be seen by the actual service organization, its current clients, or its auditors. These reports are not intended for wider or public distribution.SAS-70 audit reports have been deprecated and are no longer in use, and both the SOC Type 2 and 3 reports are designed to expand upon the SOC Type 1 reports and are for broader audiences.

NEW QUESTION 217
- (Exam Topic 3)
Which of the following is NOT one of the main intended goals of a DLP solution?

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

Answer: B

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

NEW QUESTION 220
- (Exam Topic 3)
Implementing baselines on systems would take an enormous amount of time and resources if the staff had to apply them to each server, and over time, it would be almost impossible to keep all the systems in sync on an ongoing basis.
Which of the following is NOT a package that can be used for implementing and maintaining baselines across an enterprise?

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

Answer: D

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

NEW QUESTION 225
- (Exam Topic 3)

Although the REST API supports a wide variety of data formats for communications and exchange, which data formats are the most commonly used?

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

Answer: C

Explanation:
JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API and are typically implemented with caching for increased scalability and performance. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data. HTML is used for authoring web pages for consumption by web browsers

NEW QUESTION 230
- (Exam Topic 3)
The management plane is used to administer a cloud environment and perform administrative tasks across a variety of systems, but most specifically it's used with the hypervisors.
What does the management plane typically leverage for this orchestration?

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

Answer: A

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

NEW QUESTION 234
- (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 238
- (Exam Topic 3)
Which phase of the cloud data lifecycle would be the MOST appropriate for the use of DLP technologies to protect the data?

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

Answer: C

Explanation:
During the share phase, data is allowed to leave the application for consumption by other vendors, systems, or services. At this point, as the data is leaving the security controls of the application, the use of DLP technologies is appropriate to control how the data is used or to force expiration. During the use, create, and store phases, traditional security controls are available and are more appropriate because the data is still internal to the application.

NEW QUESTION 243
- (Exam Topic 3)
Many aspects and features of cloud computing can make eDiscovery compliance more difficult or costly. Which aspect of cloud computing would be the MOST complicating factor?

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

Answer: C

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

NEW QUESTION 246
- (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 250
- (Exam Topic 3)
From the perspective of compliance, what is the most important consideration when it comes to data center location?

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

Answer: C

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

NEW QUESTION 255
- (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 257
- (Exam Topic 2)
Which of the following is NOT a domain of the Cloud Controls Matrix (CCM)?

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

Answer: D

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

NEW QUESTION 259
- (Exam Topic 2)
What changes are necessary to application code in order to implement DNSSEC?

A. Adding encryption modules
B. Implementing certificate validations
C. Additional DNS lookups
D. No changes are needed.

Answer: D

Explanation:
To implement DNSSEC, no additional changes are needed to applications or their code because the integrity checks are all performed at the system level.

NEW QUESTION 264
- (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 266
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the requirements placed on a system or application by law, policy, or requirements from standards?

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

Answer: A

Explanation:
Regulatory requirements are those imposed upon businesses and their operations either by law, regulation, policy, or standards and guidelines. These requirements are specific either to the locality in which the company or application is based or to the specific nature of the data and transactions conducted.

NEW QUESTION 271
- (Exam Topic 2)
Which of the following is NOT a function performed by the handshake protocol of TLS?

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

Answer: B

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

NEW QUESTION 276
- (Exam Topic 2)
Which of the following is the sole responsibility of the cloud provider, regardless of which cloud model is used?

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

Answer: C

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

NEW QUESTION 280
- (Exam Topic 2)
Which approach is typically the most efficient method to use for data discovery?

A. Metadata
B. Content analysis
C. Labels

D. ACLs

Answer: A

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

NEW QUESTION 285
- (Exam Topic 2)
Which of the cloud deployment models requires the cloud customer to be part of a specific group or organization in order to host cloud services within it?

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

Answer: A

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

NEW QUESTION 290
- (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 294
- (Exam Topic 2)
Which of the following is NOT part of a retention policy?

A. Format
B. Costs
C. Accessibility
D. Duration

Answer: B

Explanation:
The data retention policy covers the duration, format, technologies, protection, and accessibility of archives, but does not address the specific costs of its implementation and maintenance.

NEW QUESTION 298
- (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 303
- (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 306
- (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 310
- (Exam Topic 2)
Which of the following is the MOST important requirement and guidance for testing during an audit?

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

Answer: D

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

NEW QUESTION 313
- (Exam Topic 2)
How many additional DNS queries are needed when DNSSEC integrity checks are added?

A. Three
B. Zero
C. One
D. Two

Answer: B

Explanation:
DNSSEC does not require any additional DNS queries to be performed. The DNSSEC integrity checks and validations are all performed as part of the single DNS lookup resolution.

NEW QUESTION 315
- (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 317
- (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 321
- (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 323
- (Exam Topic 2)
Which of the cloud deployment models offers the most control and input to the cloud customer as to how the overall cloud environment is implemented and configured?

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

Answer: D

Explanation:
A private cloud model, and the specific contractual relationships involved, will give a cloud customer the most level of input and control over how the overall cloud environment is designed and implemented. This would be even more so in cases where the private cloud is owned and operated by the same organization that is hosting services within it.

NEW QUESTION 326
- (Exam Topic 2)
What strategy involves replacing sensitive data with opaque values, usually with a means of mapping it back to the original value?

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

Answer: C

Explanation:
Tokenization is the practice of utilizing a random and opaque "token" value in data to replace what otherwise would be a sensitive or protected data object. The token value is usually generated by the application with a means to map it back to the actual real value, and then the token value is placed in the data set with the same formatting and requirements of the actual real value so that the application can continue to function without different modifications or code changes.

NEW QUESTION 327
- (Exam Topic 2)
What does static application security testing (SAST) offer as a tool to the testers?

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

Answer: C

Explanation:
Static application security testing (SAST) is conducted with knowledge of the system, including source code, and is done against offline systems.

NEW QUESTION 329
- (Exam Topic 2)
Which data point that auditors always desire is very difficult to provide within a cloud environment?

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

Answer: B

Explanation:

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

NEW QUESTION 330
- (Exam Topic 2)
Which of the following is NOT something that an HIDS will monitor?

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

Answer: B

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

NEW QUESTION 333
- (Exam Topic 2)
What does the REST API use to protect data transmissions?

A. NetBIOS
B. VPN
C. Encapsulation
D. TLS

Answer: D

Explanation:
Representational State Transfer (REST) uses TLS for communication over secured channels. Although REST also supports SSL, at this point SSL has been phased out due to vulnerabilities and has been replaced by TLS.

NEW QUESTION 335
- (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 337
- (Exam Topic 2)
Which of the following service capabilities gives the cloud customer the least amount of control over configurations and deployments?

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

Answer: C

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

NEW QUESTION 339
- (Exam Topic 1)
What is the biggest concern with hosting a key management system outside of the cloud environment?

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

Answer: C

Explanation:
When a key management system is outside of the cloud environment hosting the application, availability is a primary concern because any access issues with the encryption keys will render the entire application unusable.

NEW QUESTION 343
- (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 346
- (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 351
- (Exam Topic 1)
Which aspect of archiving must be tested regularly for the duration of retention requirements?

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

Answer: B

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

NEW QUESTION 352
- (Exam Topic 1)
What is the data encapsulation used with the SOAP protocol referred to?

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

Answer: B

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

NEW QUESTION 357
- (Exam Topic 1)
Which of the following statements accurately describes VLANs?

A. They are not restricted to the same data center or the same racks.
B. They are not restricted to the name rack but restricted to the same data center.
C. They are restricted to the same racks and data centers.
D. They are not restricted to the same rack but restricted to same switches.

Answer: A

Explanation:
A virtual area network (VLAN) can span any networks within a data center, or it can span across different physical locations and data centers.

NEW QUESTION 361
- (Exam Topic 1)
Which term relates to the application of scientific methods and practices to evidence?

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

Answer: A

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

NEW QUESTION 364
- (Exam Topic 1)
Which of the following represents a control on the maximum amount of resources that a single customer, virtual machine, or application can consume within a cloud environment?

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

Answer: D

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

NEW QUESTION 368
- (Exam Topic 1)
What expectation of data custodians is made much more challenging by a cloud implementation, especially with PaaS or SaaS?

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

Answer: B

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

NEW QUESTION 371
- (Exam Topic 1)
Which of the following is not a risk management framework?

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

Answer: B

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

NEW QUESTION 375
- (Exam Topic 1)
Which technology is NOT commonly used for security with data in transit?

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

Answer: A

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

NEW QUESTION 380
- (Exam Topic 1)
Which of the following is not a component of contractual PII?

A. Scope of processing

B. Value of data
C. Location of data
D. Use of subcontractors

Answer: C

Explanation:
The value of data itself has nothing to do with it being considered a part of contractual

NEW QUESTION 384
- (Exam Topic 1)
What type of masking strategy involves making a separate and distinct copy of data with masking in place?

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

Answer: C

Explanation:
With static masking, a separate and distinct copy of the data set is created with masking in place. This is typically done through a script or other process that takes a standard data set, processes it to mask the appropriate and predefined fields, and then outputs the data set as a new one with the completed masking done.

NEW QUESTION 387
- (Exam Topic 1)
Which United States law is focused on accounting and financial practices of organizations?

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

Answer: C

Explanation:
The Sarbanes-Oxley (SOX) Act is not an act that pertains to privacy or IT security directly, but rather regulates accounting and financial practices used by organizations. It was passed to protect stakeholders and shareholders from improper practices and errors, and it sets forth rules for compliance, regulated and enforced by the Securities and Exchange Commission (SEC). The main influence on IT systems and operations is the requirements it sets for data retention, specifically in regard to what types of records must be preserved and for how long.

NEW QUESTION 391
- (Exam Topic 1)
Which of the following roles involves overseeing billing, purchasing, and requesting audit reports for an organization within a cloud environment?

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

Answer: B

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

NEW QUESTION 392
- (Exam Topic 1)
Which of the following concepts refers to a cloud customer paying only for the resources and offerings they use within a cloud environment, and only for the duration that they are consuming them?

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

Answer: B

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

NEW QUESTION 394
- (Exam Topic 1)
Which networking concept in a cloud environment allows for network segregation and isolation of IP spaces?

A. PLAN

B. WAN
C. LAN
D. VLAN

Answer: D

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

NEW QUESTION 396
- (Exam Topic 1)
Which of the following roles involves the provisioning and delivery of cloud services?

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

Answer: C

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

NEW QUESTION 397
- (Exam Topic 1)
Which of the following threat types can occur when encryption is not properly applied or insecure transport mechanisms are used?

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

Answer: C

Explanation:
Sensitive data exposure occurs when information is not properly secured through encryption and secure transport mechanisms; it can quickly become an easy and broad method for attackers to compromise information. Web applications must enforce strong encryption and security controls on the application side, but secure methods of communications with browsers or other clients used to access the information are also required. Security misconfiguration occurs when applications and systems are not properly configured for security, often a result of misapplied or inadequate baselines. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, thus allowing spoofing for malware or phishing attacks.

NEW QUESTION 399
- (Exam Topic 1)
Which of the following are the storage types associated with PaaS?

A. Structured and freeform
B. Volume and object
C. Structured and unstructured
D. Database and file system

Answer: C

NEW QUESTION 403
- (Exam Topic 1)
Which data formats are most commonly used with the REST API?

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

Answer: C

Explanation:
JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API, and are typically implemented with caching for increased scalability and performance.

NEW QUESTION 405
- (Exam Topic 1)
Which of the following are the storage types associated with IaaS?

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

Answer: A

NEW QUESTION 408
.....

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