

Exam Questions CCSP

Certified Cloud Security Professional

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



NEW QUESTION 1

- (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 2

- (Exam Topic 4)

Which of the following storage types is most closely associated with a database-type storage implementation?

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

Answer: D

Explanation:

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

NEW QUESTION 3

- (Exam Topic 4)

Which of the following is the best example of a key component of regulated PII?

- A. Audit rights of subcontractors
- B. Items that should be implemented
- C. PCI DSS
- D. Mandatory breach reporting

Answer: D

Explanation:

Mandatory breach reporting is the best example of regulated PII components. The rest are generally considered components of contractual PII.

NEW QUESTION 4

- (Exam Topic 4)

Which cloud service category most commonly uses client-side key management systems?

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

Answer: A

Explanation:

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

NEW QUESTION 5

- (Exam Topic 4)

Which ITIL component is an ongoing, iterative process of tracking all deployed and configured resources that an organization uses and depends on, whether they are hosted in a traditional data center or a cloud?

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

Answer: D

Explanation:

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

NEW QUESTION 6

- (Exam Topic 4)

Which of the following concepts is NOT one of the core components to an encryption system architecture?

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

Answer: B

Explanation:

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

NEW QUESTION 7

- (Exam Topic 4)

What type of masking would you employ to produce a separate data set for testing purposes based on production data without any sensitive information?

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

Answer: D

Explanation:

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

NEW QUESTION 8

- (Exam Topic 4)

Which ITIL component focuses on ensuring that system resources, processes, and personnel are properly allocated to meet SLA requirements?

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

Answer: B

Explanation:

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

NEW QUESTION 9

- (Exam Topic 4)

With the rapid emergence of cloud computing, very few regulations were in place that pertained to it specifically, and organizations often had to resort to using a collection of regulations that were not specific to cloud in order to drive audits and policies.

Which standard from the ISO/IEC was designed specifically for cloud computing?

- A. ISO/IEC 27001
- B. ISO/IEC 19889
- C. ISO/IEC 27001:2015
- D. ISO/IEC 27018

Answer: D

Explanation:

ISO/IEC 27018 was implemented to address the protection of personal and sensitive information within a cloud environment. ISO/IEC 27001 and its later 27001:2015 revision are both general-purpose data security standards. ISO/IEC 19889 is an erroneous answer.

NEW QUESTION 10

- (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 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 12

- (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 15

- (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 20

- (Exam Topic 4)

Tokenization requires two distinct _____.

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

Answer: D

Explanation:

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

NEW QUESTION 22

- (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 27

- (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 31

- (Exam Topic 4)

Which of the following best describes the Organizational Normative Framework (ONF)?

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

Answer: D

Explanation:

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

NEW QUESTION 35

- (Exam Topic 4)

What is the Cloud Security Alliance Cloud Controls Matrix (CCM)?

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

Answer: C

Explanation:

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

NEW QUESTION 39

- (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 41

- (Exam Topic 4)

Cloud systems are increasingly used for BCDR solutions for organizations. What aspect of cloud computing makes their use for BCDR the most attractive?

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

Answer: B

Explanation:

Business continuity and disaster recovery (BCDR) solutions largely sit idle until they are actually needed. This traditionally has led to increased costs for an organization because physical hardware must be purchased and operational but is not used. By using a cloud system, an organization will only pay for systems when they are being used and only for the duration of use, thus eliminating the need for extra hardware and costs. Portability is the ability to easily move services among different cloud providers. Broad network access allows access to users and staff from anywhere and from different clients, and although this would be important for a BCDR situation, it is not the best answer in this case. On-demand self-service allows users to provision services automatically and when needed, and although this too would be important for BCDR situations, it is not the best answer because it does not address costs or the biggest benefits to an organization.

NEW QUESTION 46

- (Exam Topic 4)

Which data sanitation method is also commonly referred to as "zeroing"?

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

Answer: A

Explanation:

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

NEW QUESTION 49

- (Exam Topic 4)

DLP solutions can aid in deterring loss due to which of the following?

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

Answer: A

Explanation:

DLP solutions may protect against inadvertent disclosure. Randomization is a technique for obscuring data, not a risk to data. DLP tools will not protect against risks from natural disasters, or against impacts due to device failure.

NEW QUESTION 52

- (Exam Topic 4)

What is an experimental technology that is intended to create the possibility of processing encrypted data without having to decrypt it first?

- A. Quantum-state
- B. Polyinstantiation
- C. Homomorphic
- D. Gastronomic

Answer: C

Explanation:

Homomorphic encryption hopes to achieve that goal; the other options are terms that have almost nothing to do with encryption.

NEW QUESTION 54

- (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 56

- (Exam Topic 4)

What concept does the D represent within the STRIDE threat model?

- A. Denial of service
- B. Distributed
- C. Data breach

D. Data loss

Answer: A

Explanation:

Any application can be a possible target of denial of service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for unauthenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks. None of the other options provided is the correct term.

NEW QUESTION 60

- (Exam Topic 4)

All the following are data analytics modes, except:

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

Answer: C

Explanation:

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

NEW QUESTION 61

- (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 64

- (Exam Topic 4)

Which of the following jurisdictions lacks a comprehensive national policy on data privacy and the protection of personally identifiable information (PII)?

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

Answer: C

Explanation:

The United States has a myriad of regulations focused on specific types of data, such as healthcare and financial, but lacks an overall comprehensive privacy law on the national level. The European Union, the Asian-Pacific Economic Cooperation, and Russia all have national privacy protections and regulations for the handling the PII data of their citizens.

NEW QUESTION 65

- (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 70

- (Exam Topic 4)

Hardening the operating system refers to all of the following except:

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

Answer: C

Explanation:

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

NEW QUESTION 71

- (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 75

- (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 77

- (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 82

- (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 85

- (Exam Topic 4)

Because of multitenancy, specific risks in the public cloud that don't exist in the other cloud service models include all the following except:

- A. DoS/DDoS
- B. Information bleed
- C. Risk of loss/disclosure due to legal seizures
- D. Escalation of privilege

Answer: A

Explanation:

DoS/DDoS threats and risks are not unique to the public cloud model.

NEW QUESTION 87

- (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 92

- (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 97

- (Exam Topic 4)

What masking strategy involves the replacing of sensitive data at the time it is accessed and used as it flows between the data and application layers of a service?

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

Answer: C

Explanation:

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

NEW QUESTION 102

- (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 105

- (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 108

- (Exam Topic 4)

You need to gain approval to begin moving your company's data and systems into a cloud environment. However, your CEO has mandated the ability to easily remove your IT assets from the cloud provider as a precondition.

Which of the following cloud concepts would this pertain to?

- A. Removability
- B. Extraction
- C. Portability
- D. Reversibility

Answer: D

Explanation:

Reversibility is the cloud concept involving the ability for a cloud customer to remove all of its data and IT assets from a cloud provider. Also, processes and agreements would be in place with the cloud provider that ensure all removals have been completed fully within the agreed upon timeframe. Portability refers to the ability to easily move between different cloud providers and not be locked into a specific one. Removability and extraction are both provided as terms similar to reversibility, but neither is the official term or concept.

NEW QUESTION 111

- (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 113

- (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 114

- (Exam Topic 4)

When crafting plans and policies for data archiving, we should consider all of the following, except:

- A. The backup process
- B. Immediacy of the technology
- C. Archive location
- D. The format of the data

Answer: D

NEW QUESTION 119

- (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 123

- (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 128

- (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 130

- (Exam Topic 4)

The application normative framework is best described as which of the following?

- A. A superset of the ONF
- B. A stand-alone framework for storing security practices for the ONF
- C. The complete ONF
- D. A subnet of the ONF

Answer: D

Explanation:

Remember, there is a one-to-many ratio of ONF to ANF; each organization has one ONF and many ANFs (one for each application in the organization). Therefore, the ANF is a subset of the ONF.

NEW QUESTION 132

- (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 134

- (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 137

- (Exam Topic 4)

Which protocol, as a part of TLS, handles negotiating and establishing a connection between two parties?

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

Answer: D

Explanation:

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

NEW QUESTION 142

- (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 145

- (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 147

- (Exam Topic 4)

What are SOC 1/SOC 2/SOC 3?

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

Answer: A

Explanation:

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

NEW QUESTION 148

- (Exam Topic 4)

What are third-party providers of IAM functions for the cloud environment?

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

Answer: D

Explanation:

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

NEW QUESTION 151

- (Exam Topic 4)

On large distributed systems with pooled resources, cloud computing relies on extensive orchestration to maintain the environment and the constant provisioning of resources.

Which of the following is crucial to the orchestration and automation of networking resources within a cloud?

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

Answer: D

Explanation:

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

NEW QUESTION 156

- (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 160

- (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 161

- (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 162

- (Exam Topic 4)

DLP solutions can aid in deterring loss due to which of the following?

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

Answer: D

Explanation:

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

NEW QUESTION 165

- (Exam Topic 4)

Security is a critical yet often overlooked consideration for BCDR planning. At which stage of the planning process should security be involved?

- A. Scope definition
- B. Requirements gathering
- C. Analysis
- D. Risk assessment

Answer: A

Explanation:

Defining the scope of the plan is the very first step in the overall process. Security should be included from the very earliest stages and throughout the entire process. Bringing in security at a later stage can lead to additional costs and time delays to compensate for gaps in planning. Risk assessment, requirements gathering, and analysis are all later steps in the process, and adding in security at any of those points can potentially cause increased costs and time delays.

NEW QUESTION 167

- (Exam Topic 4)

Which of the following areas of responsibility would be shared between the cloud customer and cloud provider within the Software as a Service (SaaS) category?

- A. Data
- B. Governance
- C. Application
- D. Physical

Answer: C

Explanation:

With SaaS, the application is a shared responsibility between the cloud provider and cloud customer. Although the cloud provider is responsible for deploying, maintaining, and securing the application, the cloud customer does carry some responsibility for the configuration of users and options. Regardless of the cloud service category used, the physical environment is always the sole responsibility of the cloud provider. With all cloud service categories, the data and governance are always the sole responsibility of the cloud customer.

NEW QUESTION 172

- (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 175

- (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 178

- (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 179

- (Exam Topic 4)

Which of the following is NOT a commonly used communications method within cloud environments to secure data in transit?

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

Answer: D

Explanation:

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

NEW QUESTION 184

- (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 189

- (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 193

- (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 easily 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 198

- (Exam Topic 4)

For optimal security, trust zones are used for network segmentation and isolation. They allow for the separation of various systems and tiers, each with its own security level.

Which of the following is typically used to allow administrative personnel access to trust zones?

- A. IPSec
- B. SSH
- C. VPN
- D. TLS

Answer: C

Explanation:

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

NEW QUESTION 203

- (Exam Topic 4)

What category of PII data can carry potential fines or even criminal charges for its improper use or disclosure?

- A. Protected
- B. Legal
- C. Regulated
- D. Contractual

Answer: C

Explanation:

Regulated PII data carries legal and jurisdictional requirements, along with official penalties for its misuse or disclosure, which can be either civil or criminal in nature. Legal and protected are similar terms, but neither is the correct answer in this case. Contractual requirements can carry financial or contractual impacts for the improper use or disclosure of PII data, but not legal or criminal penalties that are officially enforced.

NEW QUESTION 208

- (Exam Topic 4)

With a federated identity system, what does the identity provider send information to after a successful authentication?

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

Answer: A

Explanation:

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

NEW QUESTION 212

- (Exam Topic 4)

Which of the following best describes the purpose and scope of ISO/IEC 27034-1?

- A. Describes international privacy standards for cloud computing
- B. Serves as a newer replacement for NIST 800-52 r4
- C. Provides an overview of network and infrastructure security designed to secure cloud applications.
- D. Provides an overview of application security that introduces definitive concepts, principles, and processes involved in application security.

Answer: D

NEW QUESTION 213

- (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 218

- (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 220

- (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 225

- (Exam Topic 4)

Which component of ITIL pertains to planning, coordinating, executing, and validating changes and rollouts to production environments?

- A. Release management
- B. Availability management
- C. Problem management
- D. Change management

Answer: A

Explanation:

Release management involves planning, coordinating, executing, and validating changes and rollouts to the production environment. Change management is a higher-level component than release management and also involves stakeholder and management approval, rather than specifically focusing the actual release itself. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION 227

- (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 230

- (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 233

- (Exam Topic 4)

What is the term we use to describe the general ease and efficiency of moving data from one cloud provider either to another cloud provider or down from the cloud?

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

Answer: D

Explanation:

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

NEW QUESTION 238

- (Exam Topic 4)

Legal controls refer to which of the following?

- A. ISO 27001
- B. PCI DSS
- C. NIST 800-53r4
- D. Controls designed to comply with laws and regulations related to the cloud environment

Answer: D

Explanation:

Legal controls are those controls that are designed to comply with laws and regulations whether they be local or international.

NEW QUESTION 239

- (Exam Topic 4)

What is the cloud service model in which the customer is responsible for administration of the OS?

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

Answer: D

Explanation:

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

NEW QUESTION 243

- (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 common 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 247

- (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 248

- (Exam Topic 4)

Which of the following is a valid risk management metric?

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

Answer: B

Explanation:

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

NEW QUESTION 249

- (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 252

- (Exam Topic 4)

Being in a cloud environment, cloud customers lose a lot of insight and knowledge as to how their data is stored and their systems are deployed.

Which concept from the ISO/IEC cloud standards relates to the necessity of the cloud provider to inform the cloud customer on these issues?

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

Answer: B

Explanation:

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

NEW QUESTION 256

- (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 261

- (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 264

- (Exam Topic 4)

Whereas a contract articulates overall priorities and requirements for a business relationship, which artifact enumerates specific compliance requirements, metrics, and response times?

- A. Service level agreement
- B. Service level contract
- C. Service compliance contract
- D. Service level amendment

Answer: A

Explanation:

The service level agreement (SLA) articulates minimum requirements for uptime, availability, processes, customer service and support, security controls, auditing requirements, and any other key aspect or requirement of the contract. Although the other choices sound similar to the correct answer, none is the proper term for this concept.

NEW QUESTION 265

- (Exam Topic 3)

Which of the following aspects of security is solely the responsibility of the cloud provider?

- A. Regulatory compliance
- B. Physical security
- C. Operating system auditing
- D. Personal security of developers

Answer: B

Explanation:

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

NEW QUESTION 268

- (Exam Topic 3)

The REST API is a widely used standard for communications of web-based services between clients and the servers hosting them.

Which protocol does the REST API depend on?

- A. HTTP
- B. SSH
- C. SAML
- D. XML

Answer: A

Explanation:

Representational State Transfer (REST) is a software architectural scheme that applies the components, connectors, and data conduits for many web applications used on the Internet. It uses and relies on the HTTP protocol and supports a variety of data formats. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data. Secure Shell client (SSH) is a secure method for allowing remote login to systems over a network.

NEW QUESTION 269

- (Exam Topic 3)

You are working for a cloud service provider and receive an eDiscovery order pertaining to one of your customers.

Which of the following would be the most appropriate action to take first?

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

Answer: D

Explanation:

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

NEW QUESTION 273

- (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 276

- (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 277

- (Exam Topic 3)

Which of the following is considered an internal redundancy for a data center?

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

Answer: B

Explanation:

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

NEW QUESTION 282

- (Exam Topic 3)

Which of the following systems is used to employ a variety of different techniques to discover and alert on threats and potential threats to systems and networks?

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

Answer: A

Explanation:

An intrusion detection system (IDS) is implemented to watch network traffic and operations, using predefined criteria or signatures, and alert administrators if anything suspect is found. An intrusion prevention system (IPS) is similar to an IDS but actually takes action against suspect traffic, whereas an IDS just alerts when it finds anything suspect. A firewall works at the network level and only takes into account IP addresses, ports, and protocols; it does not inspect the traffic for patterns or content. A web application firewall (WAF) works at the application layer and provides additional security via proxying, filtering service requests, or blocking based on additional factors such as the client and requests.

NEW QUESTION 286

- (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 287

- (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 289

- (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 291

- (Exam Topic 3)

Clustered systems can be used to ensure high availability and load balancing across individual systems through a variety of methodologies.

What process is used within a clustered system to ensure proper load balancing and to maintain the health of the overall system to provide high availability?

- A. Distributed clustering
- B. Distributed balancing
- C. Distributed optimization
- D. Distributed resource scheduling

Answer: D

Explanation:

Distributed resource scheduling (DRS) is used within all clustered systems as the method for providing high availability, scaling, management, workload distribution, and the balancing of jobs and processes. None of the other choices is the correct term in this case.

NEW QUESTION 292

- (Exam Topic 3)

Which cloud deployment model is MOST likely to offer free or very cheap services to users?

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

Answer: C

Explanation:

Public clouds offer services to anyone, regardless of affiliation, and are the most likely to offer free services to users. Examples of public clouds with free services include iCloud, Dropbox, and OneDrive. Private cloud models are designed for specific customers and for their needs, and would not offer services to the public at large, for free or otherwise. A community cloud is specific to a group of similar organizations and would not offer free or widely available public services. A hybrid cloud model would not fit the specifics of the question.

NEW QUESTION 297

- (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 300

- (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 305

- (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 308

- (Exam Topic 3)

Although host-based and network-based IDSs perform similar functions and have similar capabilities, which of the following is an advantage of a network-based IDS over a host-based IDS, assuming all capabilities are equal?

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

Answer: A

Explanation:

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

NEW QUESTION 311

- (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 314

- (Exam Topic 3)

Within a federated identity system, which of the following would you be MOST likely to use for sending information for consumption by a relying party?

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

Answer: D

Explanation:

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

NEW QUESTION 315

- (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 317

- (Exam Topic 3)

Although much of the attention given to data security is focused on keeping data private and only accessible by authorized individuals, of equal importance is the trustworthiness of the data.

Which concept encapsulates this?

- A. Validity
- B. Integrity
- C. Accessibility
- D. Confidentiality

Answer: B

Explanation:

Integrity refers to the trustworthiness of data and whether its format and values are true and have not been corrupted or otherwise altered through unauthorized means. Confidentiality refers to keeping data from being access or viewed by unauthorized parties. Accessibility means that data is available and ready when needed by a user or service. Validity can mean a variety of things that are somewhat similar to integrity, but it's not the most appropriate answer in this case.

NEW QUESTION 318

- (Exam Topic 3)

Which of the following actions will NOT make data part of the create phase of the cloud data lifecycle?

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

Answer: B

Explanation:

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

NEW QUESTION 322

- (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 324

- (Exam Topic 3)

If a company needed to guarantee through contract and SLAs that a cloud provider would always have available sufficient resources to start their services and provide a certain level of provisioning, what would the contract need to refer to?

- A. Limit
- B. Reservation
- C. Assurance
- D. Guarantee

Answer: B

Explanation:

A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources. A limit refers to the enforcement of a maximum level of resources that can be consumed by or allocated to a cloud customer, service, or system. Both guarantee and assurance are terms that sound similar to reservation, but they are not correct choices.

NEW QUESTION 327

- (Exam Topic 3)

Which cloud storage type requires special consideration on the part of the cloud customer to ensure they do not program themselves into a vendor lock-in situation?

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

Answer: D

Explanation:

Structured storage is designed, maintained, and implemented by a cloud service provider as part of a PaaS offering. It is specific to that cloud provider and the way they have opted to implement systems, so special care is required to ensure that applications are not designed in a way that will lock the cloud customer into a specific cloud provider with that dependency. Unstructured storage for auxiliary files would not lock a customer into a specific provider. With volume and object storage, because the cloud customer maintains their own systems with IaaS, moving and replicating to a different cloud provider would be very easy.

NEW QUESTION 330

- (Exam Topic 3)

Many of the traditional concepts of systems and services for a traditional data center also apply to the cloud. Both are built around key computing concepts. Which of the following compromise the two facets of computing?

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

Answer: C

Explanation:

The CPU and memory resources of an environment together comprise its "computing" resources. Cloud environments, especially public clouds, are enormous pools of resources for computing and are typically divided among a large number of customers with constantly changing needs and demands. Although storage and networking are core components of a cloud environment, they do not comprise its computing core. Software, much like within a traditional data center, is highly subjective based on the application, system, service, or cloud computing model used; however, it is not one of the core cloud components.

NEW QUESTION 331

- (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 332

- (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 337

- (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 340

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 344

- (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 349

- (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 354

- (Exam Topic 3)

Which of the following threat types involves leveraging a user's browser to send untrusted data to be executed with legitimate access via the user's valid credentials?

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

Answer: D

Explanation:

Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or perhaps the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with their own access and permissions, allowing the attacker to redirect the user's web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.

NEW QUESTION 356

- (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 359

- (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 360

- (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 363

- (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 364

- (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 365

- (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 366

- (Exam Topic 3)

Data center and operations design traditionally takes a tiered, topological approach.

Which of the following standards is focused on that approach and is prevalently used throughout the industry?

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

Answer: D

Explanation:

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

NEW QUESTION 371

- (Exam Topic 3)

Which aspect of cloud computing pertains to cloud customers only paying for the resources and services they actually use?

- A. Metered service
- B. Measured billing
- C. Metered billing
- D. Measured service

Answer: D

Explanation:

Measured service is the aspect of cloud computing that pertains to cloud services and resources being billed in a metered way, based only on the level of consumption and duration of the cloud customer. Although they sound similar to the correct answer, none of the other choices is the actual cloud terminology.

NEW QUESTION 374

- (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 378

- (Exam Topic 3)

When an API is being leveraged, it will encapsulate its data for transmission back to the requesting party or service.

What is the data encapsulation used with the SOAP protocol referred to as?

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

Answer: D

Explanation:

Simple Object Access Protocol (SOAP) encapsulates its information in what is known as a SOAP envelope. It then leverages common communications protocols for transmission. Object is a type of cloud storage, but also a commonly used term with certain types of programming languages. Packet and payload are terms that sound similar to envelope but are not correct in this case.

NEW QUESTION 379

- (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 relative humidity for data centers. None of these options is the recommendation from ASHRAE.

NEW QUESTION 382

- (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 387

- (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 388

- (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 390

- (Exam Topic 3)

Different certifications and standards take different approaches to data center design and operations. Although many traditional approaches use a tiered methodology, which of the following utilizes a macro-level approach to data center design?

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

Answer: A

Explanation:

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

NEW QUESTION 394

- (Exam Topic 3)

With an API, various features and optimizations are highly desirable to scalability, reliability, and security. What does the REST API support that the SOAP API does NOT support?

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

Answer: B

Explanation:

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

NEW QUESTION 395

- (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 397

- (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 402

- (Exam Topic 3)

With a federated identity system, where would a user perform their authentication when requesting services or application access?

- A. Cloud provider
- B. The application
- C. Their home organization
- D. Third-party authentication system

Answer: C

Explanation:

With a federated identity system, a user will perform authentication with their home organization, and the application will accept the authentication tokens and user information from the identity provider in order to grant access. The purpose of a federated system is to allow users to authenticate from their home organization. Therefore, using the application or a third-party authentication system would be contrary to the purpose of a federated system because it necessitates the creation of additional accounts. The use of a cloud provider would not be relevant to the operations of a federated system.

NEW QUESTION 404

- (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 407

- (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 408

- (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 412

- (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 413

- (Exam Topic 2)

What does the "SOC" acronym refer to with audit reports?

- A. Service Origin Confidentiality
- B. System Organization Confidentiality
- C. Service Organizational Control
- D. System Organization Control

Answer: C

NEW QUESTION 415

- (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 418

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the oversight of processes and systems, as well as to ensuring their compliance with specific policies and regulations?

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

Answer: D

Explanation:

Auditing involves reports and evidence that show user activity, compliance with controls and regulations, the systems and processes that run and what they do, as well as information and data access and modification records. A cloud environment adds additional complexity to traditional audits because the cloud customer will not have the same level of access to systems and data as they would in a traditional data center.

NEW QUESTION 420

- (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 422

- (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 423

- (Exam Topic 2)

Which type of audit report is considered a "restricted use" report for its intended audience?

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

Answer: C

Explanation:

SOC Type 1 reports are considered "restricted use" reports. They are intended for management and stakeholders of an organization, clients of the service organization, and auditors of the organization. They are not intended for release beyond those audiences.

NEW QUESTION 427

- (Exam Topic 2)

Which of the cloud deployment models offers the easiest initial setup and access for the cloud customer?

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

Answer: D

Explanation:

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

NEW QUESTION 429

- (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 433

- (Exam Topic 2)

Which security concept, if implemented correctly, will protect the data on a system, even if a malicious actor gains access to the actual system?

- A. Sandboxing
- B. Encryption
- C. Firewalls
- D. Access control

Answer: B

Explanation:

In any environment, data encryption is incredibly important to prevent unauthorized exposure of data either internally or externally. If a system is compromised by an attack, having the data encrypted on the system will prevent its unauthorized exposure or export, even with the system itself being exposed.

NEW QUESTION 434

- (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 439

- (Exam Topic 2)

What concept does the "T" represent in the STRIDE threat model?

- A. TLS
- B. Testing
- C. Tampering with data
- D. Transport

Answer: C

Explanation:

Any application that sends data to the user will face the potential that the user could manipulate or alter the data, whether it resides in cookies, GET or POST commands, or headers, or manipulates client-side validations. If the user receives data from the application, it is crucial that the application validate and verify any data that is received back from the user.

NEW QUESTION 442

- (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 446

- (Exam Topic 2)

What concept does the "D" represent with the STRIDE threat model?

- A. Data loss
- B. Denial of service
- C. Data breach
- D. Distributed

Answer: B

Explanation:

Any application can be a possible target of denial-of-service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for non-authenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks.

NEW QUESTION 451

- (Exam Topic 2)

Which of the following is a commonly used tool for maintaining system configurations?

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

Answer: C

Explanation:

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

NEW QUESTION 453

- (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 454

- (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 459

- (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 461

- (Exam Topic 2)

Which of the following service categories entails the least amount of support needed on the part of the cloud customer?

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

Answer: A

Explanation:

With SaaS providing a fully functioning application that is managed and maintained by the cloud provider, cloud customers incur the least amount of support responsibilities themselves of any service category.

NEW QUESTION 463

- (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 466

- (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 467

- (Exam Topic 2)

Which type of controls are the SOC Type 1 reports specifically focused on?

- A. Integrity
- B. PII
- C. Financial
- D. Privacy

Answer: C

Explanation:

SOC Type 1 reports are focused specifically on internal controls as they relate to financial reporting.

NEW QUESTION 472

- (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 476

- (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 477

- (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 480

.....

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