

## CCSP Dumps

### Certified Cloud Security Professional

<https://www.certleader.com/CCSP-dumps.html>



#### NEW QUESTION 1

- (Exam Topic 4)

Which of the following is considered a physical control?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 2

- (Exam Topic 4)

The cloud customer will have the most control of their data and systems, and the cloud provider will have the least amount of responsibility, in which cloud computing arrangement?

- A. IaaS
- B. SaaS
- C. Community cloud
- D. PaaS

**Answer:** A

#### Explanation:

IaaS entails the cloud customer installing and maintaining the OS, programs, and data; PaaS has the customer installing programs and data; in SaaS, the customer only uploads data. In a community cloud, data and device owners are distributed.

#### NEW QUESTION 3

- (Exam Topic 4)

BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business. Which concept pertains to the required amount of time to restore services to the predetermined level?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 4

- (Exam Topic 4)

APIs are defined as which of the following?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 5

- (Exam Topic 4)

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

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

**Answer:** A

#### Explanation:

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

**NEW QUESTION 6**

- (Exam Topic 4)

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 7**

- (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 8**

- (Exam Topic 4)

Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 9**

- (Exam Topic 4)

Which of the following provides assurance, to a predetermined acceptable level of certainty, that an entity is indeed who they claim to be?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 10**

- (Exam Topic 4)

As part of the auditing process, getting a report on the deviations between intended configurations and actual policy is often crucial for an organization. What term pertains to the process of generating such a report?

- A. Deficiencies

- B. Findings
- C. Gap analysis
- D. Errors

**Answer:** C

**Explanation:**

The gap analysis determines if there are any differences between the actual configurations in use on systems and the policies that govern what the configurations are expected or mandated to be. The other terms provided are all similar to the correct answer ("findings" in particular is often used to articulate deviations in configurations), but gap analysis is the official term used.

**NEW QUESTION 10**

- (Exam Topic 4)

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 13**

- (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 16**

- (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 21**

- (Exam Topic 4)

What is the experimental technology that might lead to the possibility of processing encrypted data without having to decrypt it first?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 26**

- (Exam Topic 4)

What type of solution is at the core of virtually all directory services?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 29**

- (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 30**

- (Exam Topic 4)

Which of the following best describes SAML?

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

**Answer:** D

**NEW QUESTION 32**

- (Exam Topic 4)

The WS-Security standards are built around all of the following standards except which one?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 36**

- (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 39**

- (Exam Topic 4)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 41**

- (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 44**

- (Exam Topic 4)

The different cloud service models have varying levels of responsibilities for functions and operations depending with the model's level of service. In which of the following models would the responsibility for patching lie predominantly with the cloud customer?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 48**

- (Exam Topic 4)

Which component of ITIL involves planning for the restoration of services after an unexpected outage or incident?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 53**

- (Exam Topic 4)

IRM solutions allow an organization to place different restrictions on data usage than would otherwise be possible through traditional security controls. Which of the following controls would be possible with IRM that would not with traditional security controls?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 54**

- (Exam Topic 4)

What are the U.S. Commerce Department controls on technology exports known as?

- A. ITAR
- B. DRM

- C. EAR
- D. EAL

**Answer:** C

**Explanation:**

EAR is a Commerce Department 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 57**

- (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 60**

- (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 62**

- (Exam Topic 4)

Different security testing methodologies offer different strategies and approaches to testing systems, requiring security personnel to determine the best type to use for their specific circumstances.

What does dynamic application security testing (DAST) NOT entail that SAST does?

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

**Answer:** B

**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 it must be discovered during its testing. As with most types of testing, dynamic application security testing (DAST) involves probing, scanning, and a discovery process for system information.

**NEW QUESTION 66**

- (Exam Topic 4)

All policies within the organization should include a section that includes all of the following, except:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 67**

- (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 68**

- (Exam Topic 4)

Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 73**

- (Exam Topic 4)

Data labels could include all the following, except:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 78**

- (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 83**

- (Exam Topic 4)

Because cloud providers will not give detailed information out about their infrastructures and practices to the general public, they will often use established auditing reports to ensure public trust, where the reputation of the auditors serves for assurance.

Which type of audit reports can be used for general public trust assurances?

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

**Answer:** C

**Explanation:**

SOC Type 3 audit reports are very similar to SOC Type 2, with the exception that they are intended for general release and public audiences. SAS-70 audits have been deprecated. SOC Type 1 audit reports have a narrow scope and are intended for very limited release, whereas SOC Type 2 audit reports are intended for wider audiences but not general release.

**NEW QUESTION 86**

- (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 88**

- (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 91**

- (Exam Topic 4)

When using a PaaS solution, what is the capability provided to the customer?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 92**

- (Exam Topic 4)

Which of the following is NOT considered a type of data loss?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 97**

- (Exam Topic 4)

The goals of SIEM solution implementation include all of the following, except:

- A. Dashboarding
- B. Performance enhancement
- C. Trend analysis
- D. Centralization of log streams

**Answer: B**

**Explanation:**

SIEM does not intend to provide any enhancement of performance; in fact, a SIEM solution may decrease performance because of additional overhead. All the rest are goals of SIEM implementations.

**NEW QUESTION 100**

- (Exam Topic 4)

Which of the following could be used as a second component of multifactor authentication if a user has an RSA token?

- A. Access card
- B. USB thumb drive
- C. Retina scan
- D. RFID

**Answer: C**

**Explanation:**

A retina scan could be used in conjunction with an RSA token because it is a biometric factor, and thus a different type of factor. An access card, RFID, and USB thumb drive are all items in possession of a user, the same as an RSA token, and as such would not be appropriate.

**NEW QUESTION 103**

- (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 105**

- (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 108**

- (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 111**

- (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 116**

- (Exam Topic 4)

Data masking can be used to provide all of the following functionality, except:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 119**

- (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 122**

- (Exam Topic 4)

In a cloud environment, encryption should be used for all the following, except:

- A. Secure sessions/VPN
- B. Long-term storage of data
- C. Near-term storage of virtualized images
- D. Profile formatting

**Answer:** D

**Explanation:**

All of these activities should incorporate encryption, except for profile formatting, which is a made-up term.

**NEW QUESTION 126**

- (Exam Topic 4)

All of these are methods of data discovery, except:

- A. Label-based
- B. User-based
- C. Content-based
- D. Metadata-based

**Answer:** B

**Explanation:**

All the others are valid methods of data discovery; user-based is a red herring with no meaning.

**NEW QUESTION 130**

- (Exam Topic 4)

Which of the following terms is not associated with cloud forensics?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 132**

- (Exam Topic 4)

Which of the following would be considered an example of insufficient due diligence leading to security or operational problems when moving to a cloud?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 134**

- (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 137**

- (Exam Topic 4)

To protect data on user devices in a BYOD environment, the organization should consider requiring all the following, except:

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 139**

- (Exam Topic 4)

The BIA can be used to provide information about all the following, except:

- A. BC/DR planning
- B. Risk analysis
- C. Secure acquisition
- D. Selection of security controls

**Answer: C**

**Explanation:**

The business impact analysis gathers asset valuation information that is beneficial for risk analysis and selection of security controls (it helps avoid putting the ten-dollar lock on the five-dollar bicycle), and criticality information that helps in BC/DR planning by letting the organization understand which systems, data, and

personnel are necessary to continuously maintain. However, it does not aid secure acquisition efforts, since the assets examined by the BIA have already been acquired.

**NEW QUESTION 143**

- (Exam Topic 4)

Many aspects of cloud computing bring enormous benefits over a traditional data center, but also introduce new challenges unique to cloud computing. Which of the following aspects of cloud computing makes appropriate data classification of high importance?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 144**

- (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 148**

- (Exam Topic 4)

What process entails taking sensitive data and removing the indirect identifiers from each data object so that the identification of a single entity would not be possible?

- A. Tokenization
- B. Encryption
- C. Anonymization
- D. Masking

**Answer:** C

**Explanation:**

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

**NEW QUESTION 150**

- (Exam Topic 4)

Maintenance mode requires all of these actions except:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 153**

- (Exam Topic 4)

User access to the cloud environment can be administered in all of the following ways except:

- A. Provider provides administration on behalf the customer

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 154**

- (Exam Topic 4)

BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.

Which concept pertains to the amount of data and services needed to reach the predetermined level of operations?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 156**

- (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 158**

- (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 161**

- (Exam Topic 4)

Countermeasures for protecting cloud operations against internal threats include all of the following except:

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

**Answer:** D

**Explanation:**

Conflict of interest is a threat, not a control.

**NEW QUESTION 164**

- (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 165**

- (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 170**

- (Exam Topic 4)

Which of the following types of data would fall under data rights management (DRM) rather than information rights management (IRM)?

- A. Personnel data
- B. Security profiles
- C. Publications
- D. Financial records

**Answer:** C

**Explanation:**

Whereas IRM is used to protect a broad range of data, DRM is focused specifically on the protection of consumer media, such as publications, music, movies, and so on. IRM is used to protect general institution data, so financial records, personnel data, and security profiles would all fall under the auspices of IRM.

**NEW QUESTION 175**

- (Exam Topic 4)

Having a reservation in a cloud environment can ensure operations continue in the event of high utilization across the cloud.

Which of the following would NOT be a capability covered by reservations?

- A. Performing business operations
- B. Starting virtual machines
- C. Running applications
- D. Auto-scaling

**Answer:** D

**Explanation:**

A reservation will not guarantee auto-scaling is available because it involves the allocation of additional resources beyond what a cloud customer already has provisioned. Reservations will guarantee minimal resources are available to start virtual machines, run applications, and perform normal business operations.

**NEW QUESTION 176**

- (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 177**

- (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 179**

- (Exam Topic 4)

Which of the following is the primary purpose of an SOC 3 report?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 181**

- (Exam Topic 4)

A comprehensive BCDR plan will encapsulate many or most of the traditional concerns of operating a system in any data center. However, what is one consideration that is often overlooked with the formulation of a BCDR plan?

- A. Availability of staff
- B. Capacity at the BCDR site
- C. Restoration of services
- D. Change management processes

**Answer: C**

**Explanation:**

BCDR planning tends to focus so much on the failing over of services in the case of a disaster that recovery back to primary hosting after the disaster is often overlooked. In many instances, this can be just as complex a process as failing over, if not more so. Availability of staff, capacity at the BCDR site, and change management processes are typically integral to BCDR plans and are common components of them.

**NEW QUESTION 183**

- (Exam Topic 4)

When beginning an audit, both the system owner and the auditors must agree on various aspects of the final audit report. Which of the following would NOT be something that is predefined as part of the audit agreement?

- A. Size
- B. Format
- C. Structure
- D. Audience

**Answer: A**

**Explanation:**

The ultimate size of the audit report is not something that would ever be included in the audit scope or definition. Decisions about the content of the report should be the only factor that drives the ultimate size of the report. The structure, audience, and format of the audit report are all crucial elements that must be defined and agreed upon as part of the audit scope.

**NEW QUESTION 187**

- (Exam Topic 4)

When using a SaaS solution, what is the capability provided to the customer?

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

program interface

I. The consumer does manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

J. To use the provider's applications running on a cloud infrastructure

K. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface

L. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

**Answer: D**

**Explanation:**

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

**NEW QUESTION 190**

- (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 195**

- (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 200**

- (Exam Topic 3)

Where is a DLP solution generally installed when utilized for monitoring data in transit?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 203**

- (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 207**

- (Exam Topic 3)

The European Union is often considered the world leader in regard to the privacy of personal data and has declared privacy to be a "human right." In what year did the EU first assert this principle?

- A. 1995
- B. 2000
- C. 2010
- D. 1999

**Answer:** A

**Explanation:**

The EU passed Directive 95/46 EC in 1995, which established data privacy as a human right. The other years listed are incorrect.

**NEW QUESTION 210**

- (Exam Topic 3)

With finite resources available within a cloud, even the largest cloud providers will at times need to determine which customers will receive additional resources first.

What is the term associated with this determination?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 212**

- (Exam Topic 3)

An SLA contains the official requirements for contract performance and satisfaction between the cloud provider and cloud customer. Which of the following would NOT be a component with measurable metrics and requirements as part of an SLA?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 214**

- (Exam Topic 3)

The president of your company has tasked you with implementing cloud services as the most efficient way of obtaining a robust disaster recovery configuration for your production services.

Which of the cloud deployment models would you MOST likely be exploring?

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

**Answer:** A

**Explanation:**

A hybrid cloud model spans two more different hosting configurations or cloud providers. This would enable an organization to continue using its current hosting configuration, while adding additional cloud services to enable disaster recovery capabilities. The other cloud deployment models--public, private, and community--would not be applicable for seeking a disaster recovery configuration where cloud services are to be leveraged for that purpose rather than production service hosting.

**NEW QUESTION 216**

- (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 221**

- (Exam Topic 3)

A DLP solution/implementation has three main components. Which of the following is NOT one of the three main components?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 226**

- (Exam Topic 3)

What does a cloud customer purchase or obtain from a cloud provider?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 229**

- (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 231**

- (Exam Topic 3)

Which cloud storage type is typically used to house virtual machine images that are used throughout the environment?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 234**

- (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 239**

- (Exam Topic 3)

Audits are either done based on the status of a system or application at a specific time or done as a study over a period of time that takes into account changes and processes.

Which of the following pairs matches an audit type that is done over time, along with the minimum span of time necessary for it?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 240**

- (Exam Topic 3)

Which of the following roles would be responsible for managing memberships in federations and the use and integration of federated services?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 245**

- (Exam Topic 3)

Within an IaaS implementation, which of the following would NOT be a metric used to quantify service charges for the cloud customer?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 246**

- (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 248**

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 252**

- (Exam Topic 3)

Along with humidity, temperature is crucial to a data center for optimal operations and protection of equipment. Which of the following is the optimal temperature range as set by ASHRAE?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 253**

- (Exam Topic 3)

What type of storage structure does object storage employ to maintain files?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 256**

- (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 261**

- (Exam Topic 3)

When dealing with PII, which category pertains to those requirements that can carry legal sanctions or penalties for failure to adequately safeguard the data and address compliance requirements?

- A. Contractual

- B. Jurisdictional
- C. Regulated
- D. Legal

**Answer:** C

**Explanation:**

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

**NEW QUESTION 265**

- (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 266**

- (Exam Topic 3)

Digital investigations have adopted many of the same methodologies and protocols as other types of criminal or scientific inquiries.

What term pertains to the application of scientific norms and protocols to digital investigations?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 267**

- (Exam Topic 3)

ISO/IEC has established international standards for many aspects of computing and any processes or procedures related to information technology.

Which ISO/IEC standard has been established to provide a framework for handling eDiscovery processes?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 269**

- (Exam Topic 3)

Different types of audits are intended for different audiences, such as internal, external, regulatory, and so on. Which of the following audits are considered "restricted use" versus being for a more broad audience?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 274**

- (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 278**

- (Exam Topic 3)

Which of the following is NOT one of the main intended goals of a DLP solution?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 281**

- (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 283**

- (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 287**

- (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 292**

- (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 296**

- (Exam Topic 3)

Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 300**

- (Exam Topic 2)

Which of the following is NOT a domain of the Cloud Controls Matrix (CCM)?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 304**

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 309**

- (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 312**

- (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 314**

- (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 317**

- (Exam Topic 2)

Which of the following is NOT a key area for performance monitoring as far as an SLA is concerned?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 319**

- (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 322**

- (Exam Topic 2)

Which value refers to the amount of data an organization would need to recover in the event of a BCDR situation in order to reach an acceptable level of operations?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 323**

- (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 324**

- (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 327**

- (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 332**

- (Exam Topic 2)

Where is an XML firewall most commonly deployed in the environment?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 333**

- (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 334**

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the requirements placed on the cloud provider by the cloud customer for minimum performance standards and requirements that must be met?

- A. Regulatory requirements
- B. SLAs
- C. Auditability
- D. Governance

**Answer:** B

**Explanation:**

Whereas a contract spells out general terms and costs for services, the SLA is where the real meat of the business relationship and concrete requirements come into play. The SLA spells out in clear terms the minimum requirements for uptime, availability, processes, customer service and support, security controls and requirements, auditing and reporting, and potentially many other areas that define the business relationship and the success of it.

**NEW QUESTION 338**

- (Exam Topic 2)

With software-defined networking, what aspect of networking is abstracted from the forwarding of traffic?

- A. Routing
- B. Session
- C. Filtering
- D. Firewalling

**Answer:** C

**Explanation:**

With software-defined networking (SDN), the filtering of network traffic is separated from the forwarding of network traffic so that it can be independently administered.

**NEW QUESTION 340**

- (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 344**

- (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 348**

- (Exam Topic 2)

What concept does the "A" represent in the DREAD model?

- A. Affected users
- B. Authentication
- C. Affinity

D. Authorization

**Answer:** A

**Explanation:**

Affected users refers to the percentage of users who would be impacted by a successful exploit. Scoring ranges from 0, which means no users are impacted, to 10, which means all users are impacted.

**NEW QUESTION 351**

- (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 355**

- (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 360**

- (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 361**

- (Exam Topic 2)

What type of masking strategy involves replacing data on a system while it passes between the data and application layers?

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

**Answer:** A

**Explanation:**

With dynamic masking, production environments are protected with the masking process being implemented between the application and data layers of the application. This allows for a masking translation to take place live in the system and during normal application processing of data.

**NEW QUESTION 365**

- (Exam Topic 2)

Which of the following is the MOST important requirement and guidance for testing during an audit?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 367**

- (Exam Topic 2)

How many additional DNS queries are needed when DNSSEC integrity checks are added?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 371**

- (Exam Topic 2)

What type of security threat is DNSSEC designed to prevent?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 374**

- (Exam Topic 2)

At which stage of the BCDR plan creation phase should security be included in discussions?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 378**

- (Exam Topic 2)

What process is used within a clustered system to provide high availability and load balancing?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 381**

- (Exam Topic 2)

What type of data does data rights management (DRM) protect?

- A. Consumer
- B. PII
- C. Financial
- D. Healthcare

**Answer:** A

**Explanation:**

DRM applies to the protection of consumer media, such as music, publications, video, movies, and soon.

**NEW QUESTION 382**

- (Exam Topic 2)

What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 386**

- (Exam Topic 2)

Which of the cloud deployment models offers the most control and input to the cloud customer as to how the overall cloud environment is implemented and configured?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 388**

- (Exam Topic 2)

What does static application security testing (SAST) offer as a tool to the testers?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 393**

- (Exam Topic 2)

Which of the following would NOT be a reason to activate a BCDR strategy?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 395**

- (Exam Topic 2)

Which of the following is NOT something that an HIDS will monitor?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 398**

- (Exam Topic 2)

What does the REST API use to protect data transmissions?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 399**

- (Exam Topic 2)

Which security concept is focused on the trustworthiness of data?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 402**

- (Exam Topic 2)

Which of the following is NOT one of the three components of a federated identity system transaction?

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

**Answer: D**

**NEW QUESTION 407**

- (Exam Topic 2)

What concept does the "R" represent with the DREAD model?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 411**

- (Exam Topic 2)

Which security concept would business continuity and disaster recovery fall under?

- A. Confidentiality
- B. Availability
- C. Fault tolerance
- D. Integrity

**Answer: B**

**Explanation:**

Disaster recovery and business continuity are vital concerns with availability. If data is destroyed or compromised, having regular backup systems in place as well as being able to perform disaster recovery in the event of a major or widespread problem allows operations to continue with an acceptable loss of time and data to management. This also ensures that sensitive data is protected and persisted in the event of the loss or corruption of data systems or physical storage systems.

**NEW QUESTION 413**

- (Exam Topic 2)

What is the concept of segregating information or processes, within the same system or application, for security reasons?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 415**

- (Exam Topic 2)

Which aspect of cloud computing makes data classification even more vital than in a traditional data center?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 417**

- (Exam Topic 2)

Which type of testing uses the same strategies and toolsets that hackers would use?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 418**

- (Exam Topic 2)

The European Union passed the first major regulation declaring data privacy to be a human right. In what year did it go into effect?

- A. 2010
- B. 2000
- C. 1995
- D. 1990

**Answer:** C

**Explanation:**

Adopted in 1995, Directive 95/46 EC establishes strong data protection and policy requirements, including the declaring of data privacy to be a human right. It establishes that an individual has the right to be notified when their personal data is being access or processed, that it only will ever be accessed for legitimate purposes, and that data will only be accessed to the exact extent it needs to be for the particular process or request.

**NEW QUESTION 419**

- (Exam Topic 1)

What is the biggest concern with hosting a key management system outside of the cloud environment?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 423**

- (Exam Topic 1)

Which of the following roles is responsible for creating cloud components and the testing and validation of services?

- A. Cloud auditor
- B. Inter-cloud provider

- C. Cloud service broker
- D. Cloud service developer

**Answer:** D

**Explanation:**

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

**NEW QUESTION 425**

- (Exam Topic 1)

Which of the following may unilaterally deem a cloud hosting model inappropriate for a system or application?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 427**

- (Exam Topic 1)

When is a virtual machine susceptible to attacks while a physical server in the same state would not be?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 429**

- (Exam Topic 1)

From a legal perspective, what is the most important first step after an eDiscovery order has been received by the cloud provider?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 431**

- (Exam Topic 1)

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

- A. Modifying metadata
- B. Importing data
- C. Modifying data
- D. Constructing new data

**Answer:** A

**Explanation:**

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

**NEW QUESTION 435**

- (Exam Topic 1)

What type of segregation and separation of resources is needed within a cloud environment for multitenancy purposes versus a traditional data center model?

- A. Virtual
- B. Security
- C. Physical

D. Logical

**Answer:** D

**Explanation:**

Cloud environments lack the ability to physically separate resources like a traditional data center can. To compensate, cloud computing logical segregation concepts are employed. These include VLANs, sandboxing, and the use of virtual network devices such as firewalls.

**NEW QUESTION 438**

- (Exam Topic 1)

What is the biggest negative to leasing space in a data center versus building or maintain your own?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 439**

- (Exam Topic 1)

Which of the following pertains to a macro level approach to data center design rather than the traditional tiered approach to data centers?

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

**Answer:** A

**Explanation:**

The standards put out by the International Data Center Authority (IDCA) have established the Infinity Paradigm, which is intended to be a comprehensive data center design and operations framework. The Infinity Paradigm shifts away from many models that rely on tiered architecture for data centers, where each successive tier increases redundancy. Instead, it emphasizes data centers being approached at a macro level, without a specific and isolated focus on certain aspects to achieve tier status.

**NEW QUESTION 442**

- (Exam Topic 1)

What type of PII is regulated based on the type of application or per the conditions of the specific hosting agreement?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 445**

- (Exam Topic 1)

Which of the following roles involves the connection and integration of existing systems and services to a cloud environment?

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

**Answer:** D

**Explanation:**

The cloud service integrator is the official role that involves connecting and integrating existing systems and services with a cloud environment. This may involve moving services into a cloud environment, or connecting to external cloud services and capabilities from traditional data center-hosted services.

**NEW QUESTION 447**

- (Exam Topic 1)

Which of the following roles is responsible for preparing systems for the cloud, administering and monitoring services, and managing inventory and assets?

- A. Cloud service business manager
- B. Cloud service deployment manager

- C. Cloud service operations manager
- D. Cloud service manager

**Answer:** C

**Explanation:**

The cloud service operations manager is responsible for preparing systems for the cloud, administering and monitoring services, providing audit data as requested or required, and managing inventory and assets.

**NEW QUESTION 450**

- (Exam Topic 1)

What expectation of data custodians is made much more challenging by a cloud implementation, especially with PaaS or SaaS?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 455**

- (Exam Topic 1)

Which of the following represents a minimum guaranteed resource within a cloud environment for the cloud customer?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 456**

- (Exam Topic 1)

Which of the following does NOT relate to the hiding of sensitive data from data sets?

- A. Obfuscation
- B. Federation
- C. Masking
- D. Anonymization

**Answer:** B

**Explanation:**

Federation pertains to authenticating systems between different organizations.

**NEW QUESTION 457**

- (Exam Topic 1)

Which United States law is focused on accounting and financial practices of organizations?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 458**

- (Exam Topic 1)

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

- A. Power distribution units

- B. Network circuits
- C. Power substations
- D. Generators

**Answer:** A

**Explanation:**

Power distribution units are internal to a data center and supply power to internal components such as racks, appliances, and cooling systems. As such, they are considered an internal redundancy.

**NEW QUESTION 461**

- (Exam Topic 1)

How is an object stored within an object storage system?

- A. Key value
- B. Database
- C. LDAP
- D. Tree structure

**Answer:** A

**Explanation:**

Object storage uses a flat structure with key values to store and access objects.

**NEW QUESTION 463**

- (Exam Topic 1)

Which of the following storage types is most closely associated with a traditional file system and tree structure?

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

**Answer:** A

**Explanation:**

Volume storage works as a virtual hard drive that is attached to a virtual machine. The operating system sees the volume the same as how a traditional drive on a physical server would be seen.

**NEW QUESTION 466**

- (Exam Topic 1)

Which of the following APIs are most commonly used within a cloud environment?

- A. REST and SAML
- B. SOAP and REST
- C. REST and XML
- D. XML and SAML

**Answer:** B

**Explanation:**

Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) are the most commonly used APIs within a cloud environment. 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.

**NEW QUESTION 467**

- (Exam Topic 1)

Which is the appropriate phase of the cloud data lifecycle for determining the data's classification?

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

**Answer:** A

**Explanation:**

Any time data is created, modified, or imported, the classification needs to be evaluated and set from the earliest phase to ensure security is always properly maintained for the duration of its lifecycle.

**NEW QUESTION 471**

- (Exam Topic 1)

Which of the following are the storage types associated with PaaS?

- A. Structured and freeform
- B. Volume and object
- C. Structured and unstructured

D. Database and file system

**Answer:** C

**NEW QUESTION 474**

- (Exam Topic 1)

What does the REST API support that SOAP does NOT support?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 475**

- (Exam Topic 1)

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

- A. Power feeds to rack
- B. Generators
- C. Power distribution units
- D. Storage systems

**Answer:** B

**Explanation:**

Generators are considered an external redundancy to a data center. Power distribution units (PDUs), storage systems, and power feeds to racks are all internal to a data center, and as such they are considered internal redundancies.

**NEW QUESTION 477**

- (Exam Topic 1)

Which data formats are most commonly used with the REST API?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 478**

- (Exam Topic 1)

Which of the following threat types involves an application developer leaving references to internal information and configurations in code that is exposed to the client?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 483**

- (Exam Topic 1)

Which of the following threat types involves an application that does not validate authorization for portions of itself after the initial checks?

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

**Answer:** B

**Explanation:**

It is imperative that an application perform checks when each function or portion of the application is accessed, to ensure that the user is properly authorized to access it. 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.

**NEW QUESTION 485**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CCSP Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CCSP-dumps.html>