

## 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)

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

Which concept pertains to the required amount of time to restore services to the predetermined level?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 3**

- (Exam Topic 4)

Countermeasures for protecting cloud operations against external attackers include all of the following except:

- A. Continual monitoring for anomalous activity.
- B. Detailed and extensive background checks.
- C. Regular and detailed configuration/change management activities
- D. Hardened devices and systems, including servers, hosts, hypervisors, and virtual machines.

**Answer:** B

**Explanation:**

Background checks are controls for attenuating potential threats from internal actors; external threats aren't likely to submit to background checks.

**NEW QUESTION 4**

- (Exam Topic 4)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 5**

- (Exam Topic 4)

In which cloud service model is the customer required to maintain the OS?

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

**Answer:** A

**Explanation:**

In IaaS, the service is bare metal, and the customer has to install the OS and the software; the customer then is responsible for maintaining that OS. In the other models, the provider installs and maintains the OS.

**NEW QUESTION 6**

- (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 7**

- (Exam Topic 4)

When data discovery is undertaken, three main approaches or strategies are commonly used to determine what the type of data, its format, and composition are for the purposes of classification.

Which of the following is NOT one of the three main approaches to data discovery?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 8**

- (Exam Topic 4)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 9**

- (Exam Topic 4)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 10**

- (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 10**

- (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 14**

- (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 19**

- (Exam Topic 4)

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

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 23**

- (Exam Topic 4)

Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 24**

- (Exam Topic 4)

Data labels could include all the following, except:

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

**Answer:** A

**Explanation:**

All the others might be included in data labels, but we don't usually include data value, since it is prone to change frequently, and because it might not be information we want to disclose to anyone who does not have need to know.

**NEW QUESTION 28**

- (Exam Topic 4)

Tokenization requires two distinct \_\_\_\_\_.

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 33**

- (Exam Topic 4)

A variety of security systems can be integrated within a network--some that just monitor for threats and issue alerts, and others that take action based on signatures, behavior, and other types of rules to actively stop potential threats.

Which of the following types of technologies is best described here?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 34**

- (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 37**

- (Exam Topic 4)

Which kind of SSAE audit report is most beneficial for a cloud customer, even though it's unlikely the cloud provider will share it?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 41**

- (Exam Topic 4)

Cryptographic keys for encrypted data stored in the cloud should be \_\_\_\_\_.

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 46**

- (Exam Topic 4)

Which of the following best describes a cloud carrier?

- A. The intermediary who provides connectivity and transport of cloud providers and cloud consumers
- B. A person or entity responsible for making a cloud service available to consumers
- C. The person or entity responsible for transporting data across the Internet
- D. The person or entity responsible for keeping cloud services running for customers

**Answer:** A

**Explanation:**

A cloud carrier is the intermediary who provides connectivity and transport of cloud services between cloud providers and cloud customers.

**NEW QUESTION 47**

- (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 52**

- (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 56**

- (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 58**

- (Exam Topic 4)

Database activity monitoring (DAM) can be:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 59**

- (Exam Topic 4)

Which of the following technologies is NOT commonly used for accessing systems and services in a cloud environment in a secure manner?

- A. KVM
- B. HTTPS
- C. VPN
- D. TLS

**Answer:** A

**Explanation:**

A keyboard-video-mouse (KVM) system is commonly used for directly accessing server terminals in a data center. It is not a method that would be possible within a cloud environment, primarily due to the use virtualized systems, but also because only the cloud provider's staff would be allowed the physical access to hardware systems that's provided by a KVM. 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.

**NEW QUESTION 61**

- (Exam Topic 4)

As a result of scandals involving publicly traded corporations such as Enron, WorldCom, and Adelphi, Congress passed legislation known as:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 66**

- (Exam Topic 4)

All the following are data analytics modes, except:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 70**

- (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 73**

- (Exam Topic 4)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 74**

- (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 75**

- (Exam Topic 4)

Limits for resource utilization can be set at different levels within a cloud environment to ensure that no particular entity can consume a level of resources that impacts other cloud customers.

Which of the following is NOT a unit covered by limits?

- A. Hypervisor
- B. Cloud customer
- C. Virtual machine
- D. Service

**Answer: A**

**Explanation:**

The hypervisor level, as a backend cloud infrastructure component, is not a unit where limits may be applied to control resource utilization. Limits can be placed at the service, virtual machine, and cloud customer levels within a cloud environment.

**NEW QUESTION 78**

- (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 80**

- (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 81**

- (Exam Topic 4)

What is one of the reasons a baseline might be changed?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 84**

- (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 87**

- (Exam Topic 4)

All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:

- A. Tokenization
- B. Masking
- C. Data discovery
- D. Obfuscation

**Answer:** C

**Explanation:**

Data discovery is a term used to describe the process of identifying information according to specific traits or categories. The rest are all methods for obscuring data.

**NEW QUESTION 91**

- (Exam Topic 4)

Data labels could include all the following, except:

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 92**

- (Exam Topic 4)

What's a potential problem when object storage versus volume storage is used within IaaS for application use and dependency?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 97**

- (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 100**

- (Exam Topic 4)

The GAPP framework was developed through a joint effort between the major Canadian and American professional accounting associations in order to assist their members with managing and preventing risks to the privacy of their data and customers. Which of the following is the meaning of GAPP?

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

**Answer:** C

**NEW QUESTION 105**

- (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 107**

- (Exam Topic 4)

When an organization is considering a cloud environment for hosting BCDR solutions, which of the following would be the greatest concern?

- A. Self-service
- B. Resource pooling
- C. Availability
- D. Location

**Answer:** D

**Explanation:**

If an organization wants to use a cloud service for BCDR, the location of the cloud hosting becomes a very important security consideration due to regulations and jurisdiction, which could be dramatically different from the organization's normal hosting locations. Availability is a hallmark of any cloud service provider, and likely will not be a prime consideration when an organization is considering using a cloud for BCDR; the same goes for self-service options. Resource pooling is common among all cloud systems and would not be a concern when an organization is dealing with the provisioning of resources during a disaster.

**NEW QUESTION 110**

- (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 112**

- (Exam Topic 4)

Which crucial aspect of cloud computing can be most threatened by insecure APIs?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 114**

- (Exam Topic 4)

A localized incident or disaster can be addressed in a cost-effective manner by using which of the following?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 117**

- (Exam Topic 4)

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

Which of the following cloud concepts would this pertain to?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 119**

- (Exam Topic 4)

The baseline should cover which of the following?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 122**

- (Exam Topic 4)

Which of the following are cloud computing roles?

- A. Cloud service broker and user
- B. Cloud customer and financial auditor
- C. CSP and backup service provider
- D. Cloud service auditor and object

**Answer:** C

**Explanation:**

The following groups form the key roles and functions associated with cloud computing. They do not constitute an exhaustive list but highlight the main roles and functions within cloud computing:

- Cloud customer: An individual or entity that utilizes or subscribes to cloud based services or resources.
- CSP: A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations or individuals, usually for a fee; otherwise known to clients “as a service.
- Cloud backup service provider: A third-party entity that manages and holds operational responsibilities for cloud-based data backup services and solutions to customers from a central data center.
- CSB: Typically a third-party entity or company that looks to extend or enhance value to multiple customers of cloud-based services through relationships with multiple CSPs. It acts as a liaison between cloud services customers and CSPs, selecting the best provider for each customer and monitoring the services. The CSB can be utilized as a “middleman” to broker the best deal and customize services to the customer’s requirements. May also resell cloud services.
- Cloud service auditor: Third-party organization that verifies attainment of SLAs.

**NEW QUESTION 123**

- (Exam Topic 4)

In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?

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

**Answer:** B

**Explanation:**

Layered defense calls for a diverse approach to security.

**NEW QUESTION 127**

- (Exam Topic 4)

What is a key capability or characteristic of PaaS?

- A. Support for a homogenous environment
- B. Support for a single programming language
- C. Ability to reduce lock-in
- D. Ability to manually scale

**Answer:** C

**Explanation:**

PaaS should have the following key capabilities and characteristics:

- Support multiple languages and frameworks: PaaS should support multiple programming languages and frameworks, thus enabling the developers to code in whichever language they prefer or the design requirements specify. In recent times, significant strides and efforts have been taken to ensure that open source stacks are both supported and utilized, thus reducing “lock-in” or issues with interoperability when changing CSPs.
- Multiple hosting environments: The ability to support a wide variety of underlying hosting environments for the platform is key to meeting customer requirements and demands. Whether public cloud, private cloud, local hypervisor, or bare metal, supporting multiple hosting environments allows the application developer or administrator to migrate the application when and as required. This can also be used as a form of contingency and continuity and to ensure the ongoing availability.
- Flexibility: Traditionally, platform providers provided features and requirements that they felt suited the client requirements, along with what suited their service offering and positioned them as the provider of choice, with limited options for the customers to move easily. This has changed drastically, with extensibility and flexibility now afforded to meeting the needs and requirements of developer audiences. This has been heavily influenced by open source, which allows relevant plug-ins to be quickly and efficiently introduced into the platform.
- Allow choice and reduce lock-in: PaaS learns from previous horror stories and restrictions, proprietary meant red tape, barriers, and restrictions on what developers could do when it came to migration or adding features and components to the platform. Although the requirement to code to specific APIs was made available by the providers, they could run their apps in various environments based on commonality and standard API structures, ensuring a level of consistency and quality for customers and users.
- Ability to auto-scale: This enables the application to seamlessly scale up and down as required to accommodate the cyclical demands of users. The platform will allocate resources and assign these to the application as required. This serves as a key driver for any seasonal organizations that experience spikes and drops in usage.

**NEW QUESTION 130**

- (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 131**

- (Exam Topic 4)

Which of the following methods of addressing risk is most associated with insurance?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 134**

- (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 137**

- (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 141**

- (Exam Topic 4)

Above and beyond general regulations for data privacy and protection, certain types of data are subjected to more rigorous regulations and oversight.

Which of the following is not a regulatory framework for more sensitive or specialized data?

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

**Answer:** A

**Explanation:**

The FIPS 140-2 standard pertains to the certification of cryptographic modules and is not a regulatory framework. The Payment Card Industry Data Security Standard (PCI DSS), the Federal Risk and Authorization Management Program (FedRAMP), and the Health Insurance Portability and Accountability Act (HIPAA) are all regulatory frameworks for sensitive or specialized data.

**NEW QUESTION 143**

- (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 147**

- (Exam Topic 4)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 152**

- (Exam Topic 4)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 157**

- (Exam Topic 4)

DLP can be combined with what other security technology to enhance data controls?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 158**

- (Exam Topic 4)

Key maintenance and security are paramount within a cloud environment due to the widespread use of encryption for both data and transmissions.

Which of the following key-management systems would provide the most robust control over and ownership of the key-management processes for the cloud customer?

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

**Answer:** A

**Explanation:**

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



**NEW QUESTION 162**

- (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 167**

- (Exam Topic 4)

Proper implementation of DLP solutions for successful function requires which of the following?

- A. Physical access limitations
- B. USB connectivity
- C. Accurate data categorization
- D. Physical presence

**Answer:** C

**Explanation:**

DLP tools need to be aware of which information to monitor and which requires categorization (usually done upon data creation, by the data owners). DLPs can be implemented with or without physical access or presence. USB connectivity has nothing to do with DLP solutions.

**NEW QUESTION 172**

- (Exam Topic 4)

Which of the following is NOT one of the components of multifactor authentication?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 174**

- (Exam Topic 4)

Which of the following are considered to be the building blocks of cloud computing?

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

**Answer:** A

**NEW QUESTION 178**

- (Exam Topic 4)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 182**

- (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 185**

- (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 188**

- (Exam Topic 4)

Which of the following statements about Type 1 hypervisors is true?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 191**

- (Exam Topic 4)

When reviewing the BIA after a cloud migration, the organization should take into account new factors related to data breach impacts. One of these new factors is:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 193**

- (Exam Topic 4)

Identity and access management (IAM) is a security discipline that ensures which of the following?

- A. That all users are properly authorized
- B. That the right individual gets access to the right resources at the right time for the right reasons.
- C. That all users are properly authenticated
- D. That unauthorized users will get access to the right resources at the right time for the right reasons

**Answer:** B

**Explanation:**

Options A and C are also correct, but included in B, making B the best choice. D is incorrect, because we don't want unauthorized users gaining access.

**NEW QUESTION 197**

- (Exam Topic 4)

When using an IaaS solution, what is the capability provided to the customer?

- A. To provision processing, storage, networks, and other fundamental computing resources when the consumer is able to deploy and run arbitrary software, which can include OSs and applications.
- B. To provision processing, storage, networks, and other fundamental computing resources when the auditor is able to deploy and run arbitrary software, which

can include OSs and applications.

C. To provision processing, storage, networks, and other fundamental computing resources when the provider is able to deploy and run arbitrary software, which can include OSs and applications.

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 199**

- (Exam Topic 4)

DLP can be combined with what other security technology to enhance data controls?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 200**

- (Exam Topic 4)

Which aspect of data poses the biggest challenge to using automated tools for data discovery and programmatic data classification?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 203**

- (Exam Topic 4)

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

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

**Answer:** C

**Explanation:**

Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discovery potential vulnerabilities. Although the term malicious captures much of the intent of penetration testing from the perspective of an attacker, it is not the best answer. Static and dynamic are two types of system testing--where static is done offline and with knowledge of the system, and dynamic is done on a live system without any previous knowledge is associated--but neither describes the type of testing being asked for in the question.

**NEW QUESTION 205**

- (Exam Topic 4)

Without the extensive funds of a large corporation, a small-sized company could gain considerable and cost-effective services for which of the following concepts by moving to a cloud environment?

- A. Regulatory
- B. Security
- C. Testing
- D. Development

**Answer:** B

**Explanation:**

Cloud environments, regardless of the specific deployment model used, have extensive and robust security

controls in place, especially in regard to physical and infrastructure security. A small company can leverage the extensive security controls and monitoring provided by a cloud provider, which they would unlikely ever be able to afford on their own. Moving to a cloud would not result in any gains for development and testing because these areas require the same rigor regardless of where deployment and hosting occur. Regulatory compliance in a cloud would not be a gain for an organization because it would likely result in additional oversight and auditing as well as require the organization to adapt to a new environment.

**NEW QUESTION 209**

- (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 211**

- (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 214**

- (Exam Topic 4)

In a federated identity arrangement using a trusted third-party model, who is the identity provider and who is the relying party?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 219**

- (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 221**

- (Exam Topic 4)

Which of the following is the dominant driver behind the regulations to which a system or application must adhere?

- A. Data source
- B. Locality
- C. Contract
- D. SLA

**Answer: B**

**Explanation:**

The locality--or physical location and jurisdiction where the system or data resides--is the dominant driver of regulations. This may be based on the type of data contained within the application or the way in which the data is used. The contract and SLA both articulate requirements for regulatory compliance and the responsibilities for the cloud provider and cloud customer, but neither artifact defines the actual requirements. Instead, the contract and SLA merely form the official documentation between the cloud provider and cloud customer. The source of the data may place contractual requirements or best practice guidelines on its usage, but ultimately jurisdiction has legal force and greater authority.

**NEW QUESTION 226**

- (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 227**

- (Exam Topic 4)

Just like the risk management process, the BCDR planning process has a defined sequence of steps and processes to follow to ensure the production of a comprehensive and successful plan.

Which of the following is the correct sequence of steps for a BCDR plan?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 230**

- (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 233**

- (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 236**

- (Exam Topic 4)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 238**

- (Exam Topic 4)

When an organization is considering the use of cloud services for BCDR planning and solutions, which of the following cloud concepts would be the most important?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 243**

- (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 247**

- (Exam Topic 4)

Which of the following is not an example of a highly regulated environment?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 249**

- (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 253**

- (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 258**

- (Exam Topic 4)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 262**

- (Exam Topic 4)

Which of the following is the least challenging with regard to eDiscovery in the cloud?

- A. Identifying roles such as data owner, controller and processor
- B. Decentralization of data storage
- C. Forensic analysis
- D. Complexities of International law

**Answer:** C

**Explanation:**

Forensic analysis is the least challenging of the answers provided as it refers to the analysis of data once it is obtained. The challenges revolve around obtaining the data for analysis due to the complexities of international law, the decentralization of data storage or difficulty knowing where to look, and identifying the data owner, controller, and processor.

**NEW QUESTION 264**

- (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 268**

- (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 271**

- (Exam Topic 4)

Which component of ITIL involves the creation of an RFC ticket and obtaining official approvals for it?

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

**Answer:** D

**Explanation:**

The change management process involves the creation of the official Request for Change (RFC) ticket, which is used to document the change, obtain the required approvals from management and stakeholders, and track the change to completion. Release management is a subcomponent of change management, where the actual code or configuration change is put into place. Deployment management is similar to release management, but it's where changes are actually implemented on systems. Problem management is focused on the identification and mitigation of known problems and deficiencies before they are able to occur.

**NEW QUESTION 272**

- (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 274**

- (Exam Topic 4)

Which of the following is not a risk management framework?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 279**

- (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 281**

- (Exam Topic 4)

Which of the following is considered an administrative control?

- A. Keystroke logging
- B. Access control process
- C. Door locks

D. Biometric authentication

**Answer:** B

**Explanation:**

A process is an administrative control; sometimes, the process includes elements of other types of controls (in this case, the access control mechanism might be a technical control, or it might be a physical control), but the process itself is administrative. Keystroke logging is a technical control (or an attack, if done for malicious purposes, and not for auditing); door locks are a physical control; and biometric authentication is a technological control.

**NEW QUESTION 283**

- (Exam Topic 4)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 285**

- (Exam Topic 4)

Every security program and process should have which of the following?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 287**

- (Exam Topic 4)

Which is the lowest level of the CSA STAR program?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 290**

- (Exam Topic 4)

Which of the following terms is NOT a commonly used category of risk acceptance?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 291**

- (Exam Topic 4)

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

- A. Service level agreement
- B. Service level contract

- C. Service compliance contract
- D. Service level amendment

**Answer:** A

**Explanation:**

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

**NEW QUESTION 292**

- (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 295**

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 298**

- (Exam Topic 4)

Which of the following is NOT one of the official risk rating categories?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 303**

- (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 304**

- (Exam Topic 3)

You are working for a cloud service provider and receive an eDiscovery order pertaining to one of your customers. Which of the following would be the most appropriate action to take first?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 307**

- (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 312**

- (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 316**

- (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 321**

- (Exam Topic 3)

With a cloud service category where the cloud customer is provided a full application framework into which to deploy their code and services, which storage types are MOST likely to be available to them?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 326**

- (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 328**

- (Exam Topic 3)

For service provisioning and support, what is the ideal amount of interaction between a cloud customer and cloud provider?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 331**

- (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 335**

- (Exam Topic 3)

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

- A. Segregated from host systems



- B. Network access
- C. Scalability
- D. External to system patching

**Answer:** A

**Explanation:**

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

**NEW QUESTION 337**

- (Exam Topic 3)

In order to prevent cloud customers from potentially consuming enormous amounts of resources within a cloud environment and thus having a negative impact on other customers, what concept is commonly used by a cloud provider?

- A. Limit
- B. Cap
- C. Throttle
- D. Reservation

**Answer:** A

**Explanation:**

A limit puts a maximum value on the amount of resources that may be consumed by either a system, a service, or a cloud customer. It is commonly used to prevent one entity from consuming enormous amounts of resources and having an operational impact on other tenants within the same cloud system. Limits can either be hard or somewhat flexible, meaning a customer can borrow from other customers while still having their actual limit preserved. A reservation is a guarantee to a cloud customer that a certain level of resources will always be available to them, regardless of what operational demands are currently placed on the cloud environment. Both cap and throttle are terms that sound similar to limit, but they are not the correct terms in this case.

**NEW QUESTION 341**

- (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 346**

- (Exam Topic 3)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 351**

- (Exam Topic 3)

Within a federated identity system, which entity accepts tokens from the identity provider?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 352**

- (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 357**

- (Exam Topic 3)

Which of the following threat types involves an application that does not validate authorization for portions of itself beyond when the user first enters it?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 361**

- (Exam Topic 3)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 363**

- (Exam Topic 3)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 367**

- (Exam Topic 3)

Many of the traditional concepts of systems and services for a traditional data center also apply to the cloud. Both are built around key computing concepts.

Which of the following compromise the two facets of computing?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 369**

- (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 371**

- (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 373**

- (Exam Topic 3)

From a security perspective, what component of a cloud computing infrastructure represents the biggest concern?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 377**

- (Exam Topic 3)

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

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

**Answer:** D

**Explanation:**

Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or perhaps the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with their

own access and permissions, allowing the attacker to redirect the user's web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.

**NEW QUESTION 378**

- (Exam Topic 3)

The share phase of the cloud data lifecycle involves allowing data to leave the application, to be shared with external systems, services, or even other vendors/contractors.

What technology would be useful for protecting data at this point?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 381**

- (Exam Topic 3)

Firewalls are used to provide network security throughout an enterprise and to control what information can be accessed--and to a certain extent, through what means.

Which of the following is NOT something that firewalls are concerned with?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 385**

- (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 386**

- (Exam Topic 3)

In order to comply with regulatory requirements, which of the following secure erasure methods would be available to a cloud customer using volume storage within the IaaS service model?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 390**

- (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 395**

- (Exam Topic 3)

One of the main components of system audits is the ability to track changes over time and to match these changes with continued compliance and internal processes.

Which aspect of cloud computing makes this particular component more challenging than in a traditional data center?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 396**

- (Exam Topic 3)

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

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 397**

- (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 401**

- (Exam Topic 3)

Within a SaaS environment, what is the responsibility on the part of the cloud customer in regard to procuring the software used?



- A. Maintenance
- B. Licensing
- C. Development
- D. Purchasing

**Answer:** B

**Explanation:**

Within a SaaS implementation, the cloud customer licenses the use of the software from the cloud provider because SaaS delivers a fully functional application to the customer. With SaaS, the cloud provider is responsible for the entire software application and any necessary infrastructure to develop, run, and maintain it. The purchasing, development, and maintenance are fully the responsibility of the cloud provider.

**NEW QUESTION 404**

- (Exam Topic 3)

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

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 406**

- (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 411**

- (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 412**

- (Exam Topic 3)

Humidity levels for a data center are a prime concern for maintaining electrical and computing resources properly as well as ensuring that conditions are optimal for top performance.

Which of the following is the optimal humidity level, as established by ASHRAE?

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

**Answer:** C

**Explanation:**



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

**NEW QUESTION 417**

- (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 419**

- (Exam Topic 3)

Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.

Which of the following is NOT a regulatory system from the United States federal government?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 421**

- (Exam Topic 3)

You were recently hired as a project manager at a major university to implement cloud services for the academic and administrative systems. Because the load and demand for services at a university are very cyclical in nature, commensurate with the academic calendar, which of the following aspects of cloud computing would NOT be a primary benefit to you?

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

**Answer: B**

**Explanation:**

Broad network access to cloud services, although it is an integral aspect of cloud computing, would not be a specific benefit to an organization with cyclical business needs. The other options would allow for lower costs during periods of low usage as well as provide the ability to expand services quickly and easily when needed for peak periods. Measured service allows a cloud customer to only use the resources it needs at the time, and resource pooling allows a cloud customer to access resources as needed. On-demand self-service enables the cloud customer to change its provisioned resources on its own, without the need to interact with the staff from the cloud provider.

**NEW QUESTION 424**

- (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 426**

- (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 430**

- (Exam Topic 3)

Which aspect of SaaS will alleviate much of the time and energy organizations spend on compliance (specifically baselines)?

- A. Maintenance
- B. Licensing
- C. Standardization
- D. Development

**Answer:** C

**Explanation:**

With the entire software platform being controlled by the cloud provider, the standardization of configurations and versioning is done automatically for the cloud customer. This alleviates the customer's need to track upgrades and releases for its own systems and development; instead, the onus is on the cloud provider. Although licensing is the responsibility of the cloud customer within SaaS, it does not have an impact on compliance requirements. Within SaaS, development and maintenance of the system are solely the responsibility of the cloud provider.

**NEW QUESTION 431**

- (Exam Topic 3)

Which phase of the cloud data lifecycle would be the MOST appropriate for the use of DLP technologies to protect the data?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 436**

- (Exam Topic 3)

Which cloud storage type resembles a virtual hard drive and can be utilized in the same manner and with the same type of features and capabilities?

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

**Answer:** A

**Explanation:**

Volume storage is allocated and mounted as a virtual hard drive within IaaS implementations, and it can be maintained and used the same way a traditional file system can. Object storage uses a flat structure on remote services that is accessed via opaque descriptors, structured storage resembles database storage, and unstructured storage is used to hold auxiliary files in conjunction with applications hosted within a PaaS implementation.

**NEW QUESTION 438**

- (Exam Topic 3)

Many aspects and features of cloud computing can make eDiscovery compliance more difficult or costly. Which aspect of cloud computing would be the MOST complicating factor?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 440**

- (Exam Topic 3)

If you are running an application that has strict legal requirements that the data cannot reside on systems that contain other applications or systems, which aspect of cloud computing would be prohibitive in this case?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 445**

- (Exam Topic 3)

From the perspective of compliance, what is the most important consideration when it comes to data center location?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 448**

.....

## 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>