

CCSP Dumps

Certified Cloud Security Professional

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



NEW QUESTION 1

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 2

- (Exam Topic 4)

Which of the following areas of responsibility always falls completely under the purview of the cloud provider, regardless of which cloud service category is used?

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

Answer: C

Explanation:

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

NEW QUESTION 3

- (Exam Topic 4)

APIs are defined as which of the following?

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

Answer: B

Explanation:

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

NEW QUESTION 4

- (Exam Topic 4)

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

- A. Cloud auditor
- B. Inter-cloud provider
- C. Cloud service broker
- D. Cloud service developer

Answer: D

Explanation:

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

NEW QUESTION 5

- (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 6

- (Exam Topic 4)

Which of the following is not a way to manage risk?

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

Answer: D

Explanation:

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

NEW QUESTION 7

- (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 8

- (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 9

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 10

- (Exam Topic 4)

Database activity monitoring (DAM) can be:

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

Answer:

A

Explanation:

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

NEW QUESTION 10

- (Exam Topic 4)

Which of the following frameworks focuses specifically on design implementation and management?

- A. ISO 31000:2009
- B. ISO 27017
- C. NIST 800-92
- D. HIPAA

Answer: A

Explanation:

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

NEW QUESTION 12

- (Exam Topic 4)

Which component of ITIL involves handling anything that can impact services for either internal or public users?

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

Answer: A

Explanation:

Incident management is focused on limiting the impact of disruptions to an organization's services or operations, as well as returning their state to full operational status as soon as possible. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur. Deployment management is a subcomponent of change management and is where the actual code or configuration change is put into place. Change management involves the processes and procedures that allow an organization to make changes to its IT systems and services in a controlled manner.

NEW QUESTION 14

- (Exam Topic 4)

The cloud customer's trust in the cloud provider can be enhanced by all of the following except:

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

Answer: D

Explanation:

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

NEW QUESTION 18

- (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 21

- (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 23

- (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 24

- (Exam Topic 4)

Which of the following is NOT a major regulatory framework?

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

Answer: D

Explanation:

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

NEW QUESTION 29

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 31

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 33

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 36

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 40

- (Exam Topic 4)

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 43

- (Exam Topic 4)

Which of the following report is most aligned with financial control audits?

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

Answer: C

Explanation:

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

NEW QUESTION 44

- (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 46

- (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 48

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 53

- (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 58

- (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 62

- (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 64

- (Exam Topic 4)

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

A. A superset of the ONF

B. A stand-alone framework for storing security practices for the ONF

C. The complete ONF

D. A subnet of the ONF

Answer: D

Explanation:

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

NEW QUESTION 66

- (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 67

- (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 70

- (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 73

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 75

- (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 80

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 85

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 89

- (Exam Topic 4)

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

- A. Multifactor authentication
- B. DLP agents

- C. Two-person integrity
- D. Local encryption

Answer: C

Explanation:

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

NEW QUESTION 94

- (Exam Topic 4)

A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence.

Which core concept of cloud computing is most related to vendor lock-in?

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

Answer: C

Explanation:

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

NEW QUESTION 95

- (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 98

- (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 99

- (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 103

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 107

- (Exam Topic 4)

In the cloud motif, the data owner is usually:

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

Answer: C

Explanation:

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

NEW QUESTION 109

- (Exam Topic 4)

The BC/DR kit should include all of the following except:

- A. Annotated asset inventory
- B. Flashlight
- C. Hard drives
- D. Documentation equipment

Answer: C

Explanation:

While hard drives may be useful in the kit (for instance, if they store BC/DR data such as inventory lists, baselines, and patches), they are not necessarily required. All the other items should be included.

NEW QUESTION 114

- (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 119

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 120

- (Exam Topic 4)

Your company is in the planning stages of moving applications that have large data sets to a cloud environment.

What strategy for data removal would be the MOST appropriate for you to recommend if costs and speed are primary considerations?

- A. Shredding
- B. Media destruction

- C. Cryptographic erasure
- D. Overwriting

Answer: C

Explanation:

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

NEW QUESTION 121

- (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 125

- (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 129

- (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 131

- (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 136

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 138

- (Exam Topic 3)

During which phase of the cloud data lifecycle is it possible for the classification of data to change?

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

Answer: C

Explanation:

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

NEW QUESTION 140

- (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 142

- (Exam Topic 3)

Which data state would be most likely to use digital signatures as a security protection mechanism?

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

Answer: A

Explanation:

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

NEW QUESTION 143

- (Exam Topic 3)

DNSSEC was designed to add a layer of security to the DNS protocol. Which type of attack was the DNSSEC extension designed to mitigate?

- A. Account hijacking
- B. Snooping
- C. Spoofing
- D. Data exposure

Answer: C

Explanation:

DNSSEC is an extension to the regular DNS protocol that utilizes digital signing of DNS query results, which can be verified to come from an authoritative source. This verification mitigates the ability for a rogue DNS server to be used to spoof query results and to direct users to malicious sites. DNSSEC provides for the verification of the integrity of DNS queries. It does not provide any protection from snooping or data exposure. Although it may help lessen account hijacking by preventing users from being directed to rogue sites, it cannot by itself eliminate the possibility.

NEW QUESTION 148

- (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 150

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 151

- (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 153

- (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 154

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 157

- (Exam Topic 3)

Which of the following threat types involves the sending of commands or arbitrary data through input fields in an application in an attempt to get that code executed as part of normal processing?

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

Answer: C

Explanation:

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

NEW QUESTION 160

- (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 161

- (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 164

- (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 165

- (Exam Topic 3)

Three central concepts define what type of data and information an organization is responsible for pertaining to eDiscovery.

Which of the following are the three components that comprise required disclosure?

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

Answer: D

Explanation:

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

NEW QUESTION 166

- (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 169

- (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 171

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 174

- (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 179

- (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 180

- (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 184

- (Exam Topic 3)

You just hired an outside developer to modernize some applications with new web services and functionality. In order to implement a comprehensive test platform for validation, the developer needs a data set that resembles a production data set in both size and composition.

In order to accomplish this, what type of masking would you use?

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

Answer: C

Explanation:

Static masking takes a data set and produces a copy of it, but with sensitive data fields masked. This allows for a full data set from production for testing purposes, but without any sensitive data. Dynamic masking works with a live system and is not used to produce a distinct copy. The terms "replicated" and "development" are not types of masking.

NEW QUESTION 187

- (Exam Topic 3)

Implementing baselines on systems would take an enormous amount of time and resources if the staff had to apply them to each server, and over time, it would be almost impossible to keep all the systems in sync on an ongoing basis.

Which of the following is NOT a package that can be used for implementing and maintaining baselines across an enterprise?

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

Answer: D

Explanation:

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

Chef is also a system for maintaining large groups of systems throughout an enterprise.

NEW QUESTION 190

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 192

- (Exam Topic 3)

Many tools and technologies are available for securing or monitoring data in transit within a data center, whether it is a traditional data center or a cloud. Which of the following is NOT a technology for securing data in transit?

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

Answer: C

Explanation:

DNSSEC is an extension of the normal DNS protocol that enables a system to verify the integrity of a DNS query resolution by signing it from the authoritative source and verifying the signing chain. It is not used for securing data transmissions or exchanges. HTTPS is the most common method for securing web service and data calls within a cloud, and TLS is the current standard for encrypting HTTPS traffic. VPNs are widely used for securing data transmissions and service access.

NEW QUESTION 197

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 198

- (Exam Topic 3)

The management plane is used to administer a cloud environment and perform administrative tasks across a variety of systems, but most specifically it's used with the hypervisors.

What does the management plane typically leverage for this orchestration?

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

Answer: A

Explanation:

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

NEW QUESTION 202

- (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 203

- (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 207

- (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 208

- (Exam Topic 3)

Which phase of the cloud data lifecycle represents the first instance where security controls can be implemented?

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

Answer: C

Explanation:

The store phase occurs immediately after the create phase, and as data is committed to storage structures, the first opportunity for security controls to be implemented is realized. During the create phase, the data is not yet part of a system where security controls can be applied, and although the use and share phases also entail the application of security controls, they are not the first phase where the process occurs.

NEW QUESTION 210

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 214

- (Exam Topic 3)

In order to ensure ongoing compliance with regulatory requirements, which phase of the cloud data lifecycle must be tested regularly?

- A. Archive
- B. Share
- C. Store
- D. Destroy

Answer: A

Explanation:

In order to ensure compliance with regulations, it is important for an organization to regularly test the restorability of archived data. As technologies change and older systems are deprecated, the risk rises for an organization to lose the ability to restore data from the format in which it is stored. With the destroy, store, and share phases, the currently used technologies will be sufficient for an organization's needs in an ongoing basis, so the risk that is elevated with archived data is not present.

NEW QUESTION 219

- (Exam Topic 2)

Which OSI layer does IPsec operate at?

- A. Network
- B. transport
- C. Application
- D. Presentation

Answer: A

Explanation:

A major difference between IPsec and other protocols such as TLS is that IPsec operates at the Internet network layer rather than the application layer, allowing for complete end-to-end encryption of all communications and traffic.

NEW QUESTION 224

- (Exam Topic 2)

What changes are necessary to application code in order to implement DNSSEC?

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

Answer: D

Explanation:

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

NEW QUESTION 227

- (Exam Topic 2)

Which of the following does NOT fall under the "IT" aspect of quality of service (QoS)?

- A. Applications
- B. Key performance indicators (KPIs)
- C. Services
- D. Security

Answer: B

Explanation:

KPIs fall under the "business" aspect of QoS, along with monitoring and measuring of events and business processes. Services, security, and applications are all core components and concepts of the "IT" aspect of QoS.

NEW QUESTION 232

- (Exam Topic 2)

Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?

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

Answer: D

Explanation:

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

NEW QUESTION 235

- (Exam Topic 2)

Which process serves to prove the identity and credentials of a user requesting access to an application or data?

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

Answer: B

Explanation:

Authentication is the process of proving whether the identity presented by a user is true and valid. This can be done through common mechanisms such as user ID and password combinations or with more secure methods such as multifactor authentication.

NEW QUESTION 238

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 240

- (Exam Topic 2)

Which of the cloud deployment models requires the cloud customer to be part of a specific group or organization in order to host cloud services within it?

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

Answer: A

Explanation:

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

NEW QUESTION 242

- (Exam Topic 2)

Which audit type has been largely replaced by newer approaches since 2011?

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

Answer: C

Explanation:

SAS-70 reports were replaced in 2011 with the SSAE-16 reports throughout the industry.

NEW QUESTION 246

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 247

- (Exam Topic 2)

Which of the following can be useful for protecting cloud customers from a denial-of-service (DoS) attack against another customer hosted in the same cloud?

- A. Reservations
- B. Measured service
- C. Limits
- D. Shares

Answer: A

Explanation:

Reservations ensure that a minimum level of resources will always be available to a cloud customer for them to start and operate their services. In the event of a DoS attack against one customer, they can guarantee that the other customers will still be able to operate.

NEW QUESTION 250

- (Exam Topic 2)

Which attribute of data poses the biggest challenge for data discovery?

- A. Labels
- B. Quality
- C. Volume
- D. Format

Answer: B

Explanation:

The main problem when it comes to data discovery is the quality of the data that analysis is being performed against. Data that is malformed, incorrectly stored or labeled, or incomplete makes it very difficult to use analytical tools against.

NEW QUESTION 252

- (Exam Topic 2)

Which of the following is NOT one of five principles of SOC Type 2 audits?

- A. Privacy
- B. Processing integrity
- C. Financial
- D. Security

Answer: C

Explanation:

The SOC Type 2 audits include five principles: security, privacy, processing integrity, availability, and confidentiality.

NEW QUESTION 257

- (Exam Topic 2)

Which data point that auditors always desire is very difficult to provide within a cloud environment?

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

Answer: B

Explanation:

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

NEW QUESTION 261

- (Exam Topic 2)

What is the minimum regularity for testing a BCDR plan to meet best practices?

- A. Once year
- B. Once a month
- C. Every six months
- D. When the budget allows it

Answer: A

Explanation:

Best practices and industry standards dictate that a BCDR solution should be tested at least once a year, though specific regulatory requirements may dictate more regular testing. The BCDR plan should also be tested whenever a major modification to a system occurs.

NEW QUESTION 266

- (Exam Topic 2)

Which of the following service capabilities gives the cloud customer the least amount of control over configurations and deployments?

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

Answer: C

Explanation:

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

NEW QUESTION 269

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 270

- (Exam Topic 1)

What does SDN stand for within a cloud environment?

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

Answer: B

Explanation:

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

NEW QUESTION 274

- (Exam Topic 1)

Which of the following roles is responsible for peering with other cloud services and providers?

- A. Cloud auditor
- B. Inter-cloud provider
- C. Cloud service broker
- D. Cloud service developer

Answer: B

Explanation:

The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated services.

NEW QUESTION 279

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 281

- (Exam Topic 1)

Which publication from the United States National Institute of Standards and Technology pertains to defining cloud concepts and definitions for the various core components of cloud computing?

- A. SP 800-153
- B. SP 800-145

- C. SP 800-53
- D. SP 800-40

Answer: B

Explanation:

NIST Special Publications 800-145 is titled "The NIST Definition of Cloud Computing" and contains definitions and explanations of core cloud concepts and components.

NEW QUESTION 282

- (Exam Topic 1)

Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?

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

Answer: B

Explanation:

Popular services such as iCloud, Dropbox, and OneDrive are all publicly available and are open to any user for free, with possible add-on services offered for a cost.

NEW QUESTION 284

- (Exam Topic 1)

Which of the following threat types can occur when an application does not properly validate input and can be leveraged to send users to malicious sites that appear to be legitimate?

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

Answer: A

Explanation:

Many web applications offer redirect or forward pages that send users to different, external sites. If these pages are not properly secured and validated, attackers can use the application to forward users off to sites for phishing or malware attempts. These attempts can often be more successful than direct phishing attempts because users will trust the site or application that sent them there, and they will assume it has been properly validated and approved by the trusted application's owners or operators. Security misconfiguration occurs when applications and systems are not properly configured for security--often a result of misapplied or inadequate baselines. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data.

NEW QUESTION 285

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 286

- (Exam Topic 1)

Which United States law is focused on PII as it relates to the financial industry?

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

Answer: D

Explanation:

The GLBA, as it is commonly called based on the lead sponsors and authors of the act, is officially known as "The Financial Modernization Act of 1999." It is specifically focused on PII as it relates to financial institutions. There are three specific components of it, covering various areas and use, on top of a general requirement that all financial institutions must provide all users and customers with a written copy of their privacy policies and practices, including with whom and for what reasons their information may be shared with other entities.

NEW QUESTION 287

- (Exam Topic 1)

If you're using iSCSI in a cloud environment, what must come from an external protocol or application?

- A. Kerberos support
- B. CHAP support
- C. Authentication
- D. Encryption

Answer: D

Explanation:

iSCSI does not natively support encryption, so another technology such as IPsec must be used to encrypt communications.

NEW QUESTION 288

- (Exam Topic 1)

Which of the following statements accurately describes VLANs?

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

Answer: A

Explanation:

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

NEW QUESTION 292

- (Exam Topic 1)

Which term relates to the application of scientific methods and practices to evidence?

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

Answer: A

Explanation:

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

NEW QUESTION 296

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 299

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 300

- (Exam Topic 1)

Which of the following standards primarily pertains to cabling designs and setups in a data center?

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

Answer: B

Explanation:

The standards put out by Building Industry Consulting Service International (BICSI) primarily cover complex cabling designs and setups for data centers, but also include specifications on power, energy efficiency, and hot/cold aisle setups.

NEW QUESTION 302

- (Exam Topic 1)

Which of the following is not a component of contractual PII?

- A. Scope of processing
- B. Value of data
- C. Location of data
- D. Use of subcontractors

Answer: C

Explanation:

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

NEW QUESTION 307

- (Exam Topic 1)

Which technique involves replacing values within a specific data field to protect sensitive data?

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

Answer: B

Explanation:

Masking involves replacing specific data within a data set with new values. For example, with credit card fields, as most who have ever purchased anything online can attest, nearly the entire credit card number is masked with a character such as an asterisk, with the last four digits left visible for identification and confirmation.

NEW QUESTION 312

- (Exam Topic 1)

Which type of cloud model typically presents the most challenges to a cloud customer during the "destroy" phase of the cloud data lifecycle?

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

Answer: C

Explanation:

With many SaaS implementations, data is not isolated to a particular customer but rather is part of the overall application. When it comes to data destruction, a particular challenge is ensuring that all of a customer's data is completely destroyed while not impacting the data of other customers.

NEW QUESTION 316

- (Exam Topic 1)

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

- A. Power distribution units
- B. Network circuits
- C. Power substations
- D. Generators

Answer: A

Explanation:

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

NEW QUESTION 319

- (Exam Topic 1)

Which of the following security measures done at the network layer in a traditional data center are also applicable to a cloud environment?

- A. Dedicated switches
- B. Trust zones
- C. Redundant network circuits

D. Direct connections

Answer: B

Explanation:

Trust zones can be implemented to separate systems or tiers along logical lines for great security and access controls. Each zone can then have its own security controls and monitoring based on its particular needs.

NEW QUESTION 321

- (Exam Topic 1)

Which United States law is focused on data related to health records and privacy?

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

Answer: D

Explanation:

The Health Insurance Portability and Accountability Act (HIPAA) requires the U.S. Federal Department of Health and Human Services to publish and enforce regulations pertaining to electronic health records and identifiers between patients, providers, and insurance companies. It is focused on the security controls and confidentiality of medical records, rather than the specific technologies used, so long as they meet the requirements of the regulations.

NEW QUESTION 323

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 326

- (Exam Topic 1)

Which of the following is the biggest concern or challenge with using encryption?

- A. Dependence on keys
- B. Cipher strength
- C. Efficiency
- D. Protocol standards

Answer: A

Explanation:

No matter what kind of application, system, or hosting model used, encryption is 100 percent dependent on encryption keys. Properly securing the keys and the exchange of them is the biggest and most important challenge of encryption systems.

NEW QUESTION 330

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 331

- (Exam Topic 1)

Which of the following threat types involves the sending of untrusted data to a user's browser to be executed with their own credentials and access?

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

Answer: B

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 where the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with the user's own access and permissions, allowing an attacker to redirect their 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.

NEW QUESTION 332

- (Exam Topic 1)

Which technology can be useful during the "share" phase of the cloud data lifecycle to continue to protect data as it leaves the original system and security controls?

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

Answer: C

Explanation:

Data loss prevention (DLP) can be applied to data that is leaving the security enclave to continue to enforce access restrictions and policies on other clients and systems.

NEW QUESTION 335

- (Exam Topic 1)

Which of the following security technologies is commonly used to give administrators access into trust zones within an environment?

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

Answer: A

Explanation:

Virtual private networks (VPNs) are commonly used to allow access into trust zones. Via a VPN, access can be controlled and logged and only allowed through secure channels by authorized users. It also adds an additional layer of encryption and protection to communications.

NEW QUESTION 340

- (Exam Topic 1)

What must be secured on physical hardware to prevent unauthorized access to systems?

- A. BIOS
- B. SSH
- C. RDP
- D. ALOM

Answer: A

Explanation:

BIOS is the firmware that governs the physical initiation and boot up of a piece of hardware. If it is compromised, an attacker could have access to hosted systems and make configurations changes to expose or disable some security elements on the system.

NEW QUESTION 342

.....

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>