

CCSP Dumps

Certified Cloud Security Professional

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



NEW QUESTION 1

- (Exam Topic 4)

Which of the following is considered a physical control?

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

Answer: A

Explanation:

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

NEW QUESTION 2

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 3

- (Exam Topic 4)

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)

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 6

- (Exam Topic 4)

Which of the following are distinguishing characteristics of a managed service provider?

- A. Be able to remotely monitor and manage objects for the customer and proactively maintain these objects under management.
- B. Have some form of a help desk but no NOC.
- C. Be able to remotely monitor and manage objects for the customer and reactively maintain these objects under management.
- D. Have some form of a NOC but no help desk.

Answer: A

Explanation:

According to the MSP Alliance, typically MSPs have the following distinguishing characteristics:

- Have some form of NOC service
- Have some form of help desk service
- Can remotely monitor and manage all or a majority of the objects for the customer
- Can proactively maintain the objects under management for the customer
- Can deliver these solutions with some form of predictable billing model, where the customer knows with great accuracy what her regular IT management expense will be

NEW QUESTION 7

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 8

- (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 9

- (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 10

- (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 10

- (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 13

- (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 16

- (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 21

- (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 26

- (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 27

- (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 28

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 33

- (Exam Topic 4)

In addition to battery backup, a UPS can offer which capability?

- A. Breach alert
- B. Confidentiality
- C. Communication redundancy
- D. Line conditioning

Answer: D

Explanation:

A UPS can provide line conditioning, adjusting power so that it is optimized for the devices it serves and smoothing any power fluctuations; it does not offer any of the other listed functions.

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 42

- (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)

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 49

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 53

- (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 54

- (Exam Topic 4)

Which of the following best describes SAML?

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

Answer: D

NEW QUESTION 55

- (Exam Topic 4)

Database activity monitoring (DAM) can be:

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

Answer: A

Explanation:

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

NEW QUESTION 56

- (Exam Topic 4)

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 60

- (Exam Topic 4)

Which data protection strategy would be useful for a situation where the ability to remove sensitive data from a set is needed, but a requirement to retain the ability to map back to the original values is also present?

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

Answer: B

Explanation:

Tokenization involves the replacement of sensitive data fields with key or token values, which can ultimately be mapped back to the original, sensitive data values. Masking refers to the overall approach to covering sensitive data, and 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. Encryption refers to the overall process of protecting data via key pairs and protecting confidentiality.

NEW QUESTION 62

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 64

- (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 69

- (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 73

- (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 75

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 77

- (Exam Topic 4)

Deviations from the baseline should be investigated and _____.

- A. Revealed
- B. Documented
- C. Encouraged
- D. Enforced

Answer: B

Explanation:

All deviations from the baseline should be documented, including details of the investigation and outcome. We do not enforce or encourage deviations. Presumably, we would already be aware of the deviation, so "revealing" is not a reasonable answer.

NEW QUESTION 80

- (Exam Topic 4)

An audit scope statement defines the limits and outcomes from an audit.

Which of the following would NOT be included as part of an audit scope statement?

- A. Reports
- B. Certification
- C. Billing
- D. Exclusions

Answer: C

Explanation:

Billing for an audit, or other cost-related items, would not be part of an audit scope statement and would instead be handled prior to the actual audit as part of the contract between the organization and auditors. Reports, exclusions to the scope of the audit, and required certifications on behalf of the systems or auditors are all crucial elements of an audit scope statement.

NEW QUESTION 85

- (Exam Topic 4)

Which of the following are attributes of cloud computing?

- A. Minimal management effort and shared resources
- B. High cost and unique resources
- C. Rapid provisioning and slow release of resources
- D. Limited access and service provider interaction

Answer: A

Explanation:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NEW QUESTION 88

- (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 93

- (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 95

- (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 97

- (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 101

- (Exam Topic 4)

What does static application security testing (SAST) offer as a tool to the testers that makes it unique compared to other common security testing methodologies?

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

Answer: B

Explanation:

Static application security testing (SAST) is conducted against offline systems with previous knowledge of them, including their source code. Live testing is not part of static testing but rather is associated with dynamic testing. Production system scanning is not appropriate because static testing is done against offline systems. Injection attempts are done with many different types of testing and are not unique to one particular type. It is therefore not the best answer to the question.

NEW QUESTION 106

- (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 107

- (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 110

- (Exam Topic 4)

During the course of an audit, which of the following would NOT be an input into the control requirements used as part of a gap analysis.

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

Answer: C

Explanation:

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

NEW QUESTION 112

- (Exam Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 115

- (Exam Topic 4)

Cryptographic keys should be secured _____.

- A. To a level at least as high as the data they can decrypt
- B. In vaults
- C. With two-person integrity
- D. By armed guards

Answer: A

Explanation:

The physical security of crypto keys is of some concern, but guards or vaults are not always necessary.

Two-person integrity might be a good practice for protecting keys. The best answer to this question is option A, because it is always true, whereas the remaining options depend on circumstances.

NEW QUESTION 119

- (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 121

- (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 124

- (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 128

- (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 132

- (Exam Topic 4)

Which format is the most commonly used standard for exchanging information within a federated identity system?

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

Answer: C

Explanation:

Security Assertion Markup Language (SAML) is the most common data format for information exchange within a federated identity system. It is used to transmit and exchange authentication and authorization data. XML is similar to SAML, but it's used for general-purpose data encoding and labeling and is not used for the exchange of authentication and authorization data in the way that SAML is for federated systems. JSON is used similarly to XML, as a text-based data exchange format that typically uses attribute-value pairings, but it's not used for authentication and authorization exchange. HTML is used only for encoding web pages for web browsers and is not used for data exchange--and certainly not in a federated system.

NEW QUESTION 137

- (Exam Topic 4)

For performance purposes, OS monitoring should include all of the following except:

- A. Disk space
- B. Disk I/O usage
- C. CPU usage
- D. Print spooling

Answer: D

Explanation:

Print spooling is not a metric for system performance; all the rest are.

NEW QUESTION 141

- (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 143

- (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 144

- (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 145

- (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 147

- (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 148

- (Exam Topic 4)

What are SOC 1/SOC 2/SOC 3?

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

Answer: A

Explanation:

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

NEW QUESTION 149

- (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 150

- (Exam Topic 4)

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 153

- (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 158

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 162

- (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 166

- (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 167

- (Exam Topic 4)

Gathering business requirements can aid the organization in determining all of this information about organizational assets, except:

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

Answer: D

Explanation:

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

NEW QUESTION 171

- (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 176

- (Exam Topic 4)

Upon completing a risk analysis, a company has four different approaches to addressing risk. Which approach it takes will be based on costs, available options, and adherence to any regulatory requirements from independent audits.

Which of the following groupings correctly represents the four possible approaches?

- A. Accept, avoid, transfer, mitigate
- B. Accept, deny, transfer, mitigate
- C. Accept, deny, mitigate, revise
- D. Accept, dismiss, transfer, mitigate

Answer: A

Explanation:

The four possible approaches to risk are as follows: accept (do not patch and continue with the risk), avoid (implement solutions to prevent the risk from occurring), transfer (take out insurance), and mitigate (change configurations or patch to resolve the risk). Each of these answers contains at least one incorrect approach name.

NEW QUESTION 180

- (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 184

- (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 discover 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 186

- (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 188

- (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 190

- (Exam Topic 4)

Many aspects of cloud computing bring enormous benefits over a traditional data center, but also introduce new challenges unique to cloud computing.

Which of the following aspects of cloud computing makes appropriate data classification of high importance?

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

Answer: A

Explanation:

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

NEW QUESTION 193

- (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 196

- (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 201

- (Exam Topic 4)

The various models generally available for cloud BC/DR activities include all of the following except:

- A. Private architecture, cloud backup
- B. Cloud provider, backup from another cloud provider
- C. Cloud provider, backup from same provider
- D. Cloud provider, backup from private provider

Answer: D

Explanation:

This is not a normal configuration and would not likely provide genuine benefit.

NEW QUESTION 203

- (Exam Topic 4)

Which protocol, as a part of TLS, handles the actual secure communications and transmission of data?

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

Answer: D

Explanation:

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

NEW QUESTION 204

- (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 205

- (Exam Topic 4)

Which of the following is considered a technological control?

- A. Firewall software
- B. Firing personnel
- C. Fireproof safe
- D. Fire extinguisher

Answer: A

Explanation:

A firewall is a technological control. The safe and extinguisher are physical controls and firing someone is an administrative control.

NEW QUESTION 209

- (Exam Topic 4)

There are many situations when testing a BCDR plan is appropriate or mandated. Which of the following would not be a necessary time to test a BCDR plan?

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

Answer: B

Explanation:

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

NEW QUESTION 210

- (Exam Topic 4)

In the cloud motif, the data processor is usually:

- A. The cloud customer
- B. The cloud provider
- C. The cloud access security broker
- D. The party that assigns access rights

Answer: B

Explanation:

In legal terms, when “data processor” is defined, it refers to anyone who stores, handles, moves, or manipulates data on behalf of the data owner or controller. In the cloud computing realm, this is the cloud provider.

NEW QUESTION 213

- (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 215

- (Exam Topic 4)

Legal controls refer to which of the following?

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

Answer: D

Explanation:

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

NEW QUESTION 217

- (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 219

- (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 221

- (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 224

- (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 225

- (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 227

- (Exam Topic 4)

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

- A. Cell blocking
- B. Sandboxing
- C. Pooling
- D. Fencing

Answer: B

Explanation:

Sandboxing involves the segregation and isolation of information or processes from other information or processes within the same system or application, typically for security concerns. Sandboxing is generally used for data isolation (for example, keeping different communities and populations of users isolated from others with similar data). In IT terminology, pooling typically means bringing together and consolidating resources or services, not segregating or separating them. Cell blocking and fencing are both erroneous terms.

NEW QUESTION 228

- (Exam Topic 4)

Your IT steering committee has, at a high level, approved your project to begin using cloud services. However, the committee is concerned with getting locked into

a single cloud provider and has flagged the ability to easily move between cloud providers as a top priority. It also wants to save costs by reusing components. Which cross-cutting aspect of cloud computing would be your primary focus as your project plan continues to develop and you begin to evaluate cloud providers?

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

Answer: A

Explanation:

Interoperability is ability to easily move between cloud providers, by either moving or reusing components and services. This can pertain to any cloud deployment model, and it gives organizations the ability to constantly evaluate costs and services as well as move their business to another cloud provider as needed or desired. Portability relates to the wholesale moving of services from one cloud provider to another, not necessarily the reuse of components or services for other purposes. Although resiliency is not an official concept within cloud computing, it certainly would be found throughout other topics such as elasticity, auto-scaling, and resource pooling. Scalability pertains to changing resource allocations to a service to meet current demand, either upward or downward in scope.

NEW QUESTION 230

- (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 234

- (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 237

- (Exam Topic 4)

Which of the following best describes a sandbox?

- A. An isolated space where untested code and experimentation can safely occur separate from the production environment.
- B. A space where you can safely execute malicious code to see what it does.
- C. An isolated space where transactions are protected from malicious software
- D. An isolated space where untested code and experimentation can safely occur within the production environment.

Answer: A

Explanation:

Options C and B are also correct, but A is more general and incorporates them both. D is incorrect, because sandboxing does not take place in the production environment.

NEW QUESTION 241

- (Exam Topic 4)

A UPS should have enough power to last how long?

- A. One day
- B. 12 hours
- C. Long enough for graceful shutdown
- D. 10 minutes

Answer: C

NEW QUESTION 243

- (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 245

- (Exam Topic 4)

Tokenization requires two distinct _____.

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

Answer: C

Explanation:

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

NEW QUESTION 250

- (Exam Topic 3)

The REST API is a widely used standard for communications of web-based services between clients and the servers hosting them. Which protocol does the REST API depend on?

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

Answer: A

Explanation:

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

NEW QUESTION 255

- (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 257

- (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 260

- (Exam Topic 3)

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

What is the term associated with this determination?

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

Answer: C

Explanation:

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

NEW QUESTION 261

- (Exam Topic 3)

Data centers have enormous power resources that are distributed and consumed throughout the entire facility. Which of the following standards pertains to the proper fire safety standards within that scope?

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

Answer: C

Explanation:

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 Uptime Institute publishes the most widely known and used standard for data center topologies and tiers. The International Data Center Authority (IDCA) offers the Infinity Paradigm, which takes a macro-level approach to data center design.

NEW QUESTION 262

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 265

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 269

- (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 274

- (Exam Topic 3)

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 277

- (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 280

- (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 283

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

firewall is intended to validate XML before it reaches the application. Placing the XML firewall between the presentation and application layers, between the firewall and IPS, or between the application and data layers would not serve the intended purpose.

NEW QUESTION 285

- (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 286

- (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 287

- (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 292

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 295

- (Exam Topic 3)

Your boss has tasked your team with getting your legacy systems and applications connected with new cloud-based services that management has decided are crucial to customer service and offerings.

Which role would you be assuming under this directive?

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

Answer: C

Explanation:

The cloud service integrator role is responsible for connecting and integrating existing services and applications with cloud-based 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 user is someone who consumes cloud services. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

NEW QUESTION 298

- (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 299

- (Exam Topic 3)

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

Which concept encapsulates this?

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

Answer: B

Explanation:

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

NEW QUESTION 304

- (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 307

- (Exam Topic 3)

Which of the following statements best describes a Type 1 hypervisor?

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

Answer: D

Explanation:

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

NEW QUESTION 308

- (Exam Topic 3)

In the wake of many scandals with major corporations involving fraud and the deception of investors and regulators, which of the following laws was passed to govern accounting and financial records and disclosures?

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

Answer: D

Explanation:

The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and accounting errors. The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy. The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Safe Harbor program was designed by the US government as a way for American companies to comply with European Union privacy laws.

NEW QUESTION 313

- (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 316

- (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 320

- (Exam Topic 3)

There is a large gap between the privacy laws of the United States and those of the European Union. Bridging this gap is necessary for American companies to do business with European companies and in European markets in many situations, as the American companies are required to comply with the stricter requirements. Which US program was designed to help companies overcome these differences?

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

Answer: D

Explanation:

The Safe Harbor regulations were developed by the Department of Commerce and are meant to serve as a way to bridge the gap between privacy regulations of the European Union and the United States. Due to the lack of adequate privacy laws and protection on the federal level in the US, European privacy regulations generally prohibit the exporting of PII from Europe to the United States. Participation in the Safe Harbor program is voluntary on the part of US organizations. These organizations must conform to specific requirements and policies that mirror those from the EU, thus possibly fulfilling the EU requirements for data sharing and export. This way, American businesses can be allowed to serve customers in the EU. The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy. The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and errors.

NEW QUESTION 325

- (Exam Topic 3)

Which one of the following threat types to applications and services involves the sending of requests that are invalid and manipulated through a user's client to execute commands on the application under the user's own credentials?

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

Answer: D

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 of seeing 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. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes. 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.

NEW QUESTION 328

- (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 329

- (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 330

- (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 331

- (Exam Topic 3)

With a cloud service category where the cloud customer is responsible for deploying all services, systems, and components needed for their applications, which of the following storage types are MOST likely to be available to them?

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

Answer: B

Explanation:

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

NEW QUESTION 333

- (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 334

- (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 336

- (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 339

- (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 343

- (Exam Topic 3)

A crucial decision any company must make is in regard to where it hosts the data systems it depends on. A debate exists as to whether it's best to lease space in a data center or build your own data center--and now with cloud computing, whether to purchase resources within a cloud.

What is the biggest advantage to leasing space in a data center versus procuring cloud services?

- A. Regulations
- B. Control
- C. Security
- D. Costs

Answer: B

Explanation:

When leasing space in a data center versus utilizing cloud services, a customer has a much greater control over its systems and services, from both the hardware/software perspective and the operational management perspective. Costs, regulations, and security are all prime considerations regardless of the hosting type selected. Although regulations will be the same in either hosting solution, in most instances, costs and security will be greater factors with leased space.

NEW QUESTION 345

- (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 being 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 349

- (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 351

- (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 352

- (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 353

- (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 357

- (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 361

- (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 364

- (Exam Topic 3)

Configurations and policies for a system can come from a variety of sources and take a variety of formats. Which concept pertains to the application of a set of configurations and policies that is applied to all systems or a class of systems?

- A. Hardening
- B. Leveling
- C. Baselines
- D. Standards

Answer: C

Explanation:

Baselines are a set of configurations and policies applied to all new systems or services, and they serve as the basis for deploying any other services on top of them. Although standards often form the basis for baselines, the term is applicable in this case. Hardening is the process of securing a system, often through the application of baselines. Leveling is an extraneous but similar term to baselining.

NEW QUESTION 365

- (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 369

- (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 371

- (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 372

- (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 373

- (Exam Topic 2)

Which of the following is a widely used tool for code development, branching, and collaboration?

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

Answer: A

Explanation:

GitHub is an open source tool that developers leverage for code collaboration, branching, and versioning.

NEW QUESTION 376

- (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 380

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 383

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 386

- (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 388

- (Exam Topic 2)

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

- A. Integrity
- B. Information disclosure
- C. IT security
- D. Insider threat

Answer: B

Explanation:

Perhaps the biggest concern for any user is having their personal and sensitive information disclosed by an application. There are many aspects of an application to consider with security and protecting this information, and it is very difficult for any application to fully ensure security from start to finish. The obvious focus is on security within the application itself, as well as protecting and storing the data.

NEW QUESTION 392

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 397

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Dynamic application security testing (DAST) is considered "black box" testing and begins with no inside knowledge of the application or its configurations. Everything about the application must be discovered during the testing.

NEW QUESTION 401

- (Exam Topic 2)

Which aspect of security is DNSSEC designed to ensure?

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

Answer: A

Explanation:

DNSSEC is a security extension to the regular DNS protocol and services that allows for the validation of the integrity of DNS lookups. It does not address confidentiality or availability at all. It allows for a DNS client to perform DNS lookups and validate both their origin and authority via the cryptographic signature that accompanies the DNS response.

NEW QUESTION 403

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 408

- (Exam Topic 2)

Which approach is typically the most efficient method to use for data discovery?

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

Answer: A

Explanation:

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

NEW QUESTION 412

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 417

- (Exam Topic 2)

Which of the following is NOT a function performed by the record protocol of TLS?

- A. Encryption
- B. Acceleration
- C. Authentication
- D. Compression

Answer: B

Explanation:

The record protocol of TLS performs the authentication and encryption of data packets, and in some cases compression as well. It does not perform any acceleration functions.

NEW QUESTION 420

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 421

- (Exam Topic 2)

From a security perspective, which of the following is a major concern when evaluating possible BCDR solutions?

- A. Access provisioning
- B. Auditing
- C. Jurisdictions
- D. Authorization

Answer: C

Explanation:

When a security professional is considering cloud solutions for BCDR, a top concern is the jurisdiction where the cloud systems are hosted. If the jurisdiction is different from where the production systems are hosted, they may be subjected to different regulations and controls, which would make a seamless BCDR solution far more difficult.

NEW QUESTION 424

- (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 428

- (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 429

- (Exam Topic 2)

Which of the following is NOT part of a retention policy?

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

Answer: B

Explanation:

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

NEW QUESTION 430

- (Exam Topic 2)

Which value refers to the percentage of production level restoration needed to meet BCDR objectives?

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

Answer: C

Explanation:

The recovery service level (RSL) is a percentage measure of the total typical production service level that needs to be restored to meet BCDR objectives in the case of a failure.

NEW QUESTION 434

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 436

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the assigning of jobs, tasks, and roles, as well as to ensuring they are successful and properly performed?

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

Answer: B

Explanation:

Governance at its core is the idea of assigning jobs, takes, roles, and responsibilities and ensuring they are satisfactory performed.

NEW QUESTION 437

- (Exam Topic 2)

What is a standard configuration and policy set that is applied to systems and virtual machines called?

- A. Standardization
- B. Baseline
- C. Hardening
- D. Redline

Answer: B

Explanation:

The most common and efficient manner of securing operating systems is through the use of baselines. A baseline is a standardized and understood set of base configurations and settings. When a new system is built or a new virtual machine is established, baselines will be applied to a new image to ensure the base configuration meets organizational policy and regulatory requirements.

NEW QUESTION 438

- (Exam Topic 2)

Which European Union directive pertains to personal data privacy and an individual's control over their personal data?

- A. 99/9/EC
- B. 95/46/EC
- C. 2000/1/EC
- D. 2013/27001/EC

Answer: B

Explanation:

Directive 95/46/EC is titled "On the protection of individuals with regard to the processing of personal data and on the free movement of such data."

NEW QUESTION 440

- (Exam Topic 2)

Which security concept is based on preventing unauthorized access to data while also ensuring that it is accessible to those authorized to use it?

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

Answer: C

Explanation:

The main goal of confidentiality is to ensure that sensitive information is not made available or leaked to parties that should not have access to it, while at the same time ensuring that those with appropriate need and authorization to access it can do so in a manner commensurate with their needs and confidentiality requirements.

NEW QUESTION 445

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the ability to easily move services and applications between different cloud providers?

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

Answer: C

Explanation:

Portability is the ease with which a service or application can be moved between different cloud providers. Maintaining portability gives an organization great flexibility between cloud providers and the ability to shop for better deals or offerings.

NEW QUESTION 450

- (Exam Topic 2)

Over time, what is a primary concern for data archiving?

- A. Size of archives
- B. Format of archives
- C. Recoverability
- D. Regulatory changes

Answer: C

Explanation:

Over time, maintaining the ability to restore and read archives is a primary concern for data archiving. As technologies change and new systems are brought in, it is imperative for an organization to ensure they are still able to restore and access archives for the duration of the required retention period.

NEW QUESTION 453

- (Exam Topic 2)

Which aspect of cloud computing would make the use of a cloud the most attractive as a BCDR solution?

- A. Interoperability
- B. Resource pooling
- C. Portability
- D. Measured service

Answer: D

Explanation:

Measured service means that costs are only incurred when a cloud customer is actually using cloud services. This is ideal for a business continuity and disaster recovery (BCDR) solution because it negates the need to keep hardware or resources on standby in case of a disaster. Services can be initiated when needed and without costs unless needed.

NEW QUESTION 455

- (Exam Topic 2)

Which of the following would be a reason to undertake a BCDR test?

- A. Functional change of the application
- B. Change in staff
- C. User interface overhaul of the application
- D. Change in regulations

Answer: A

Explanation:

Any time a major functional change of an application occurs, a new BCDR test should be done to ensure the overall strategy and process are still applicable and appropriate.

NEW QUESTION 460

- (Exam Topic 2)

What type of security threat is DNSSEC designed to prevent?

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

Answer: C

Explanation:

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

NEW QUESTION 464

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 468

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 469

- (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 474

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 475

- (Exam Topic 2)

What strategy involves replacing sensitive data with opaque values, usually with a means of mapping it back to the original value?

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

Answer: C

Explanation:

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

NEW QUESTION 478

.....

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>