ISC.CCSP.v2025-04-19.q608

Exam Code:	CCSP
Exam Name:	Certified Cloud Security Professional
Certification Provider:	ISC
Free Question Number:	608
Version:	v2025-04-19
# of views:	3739
# of Questions views:	6080
https://www.freepdfdumps.com/ISC.CCSP.v2025-04-19.q608.html	

NEW QUESTION: 1
Which of the following statements about Type 1 hypervisors is true?
A. The hardware vendor and software vendor are different.
B. The hardware vendor and software vendor are the same
C. The hardware vendor provides an open platform for software vendors.
D. The hardware vendor and software vendor should always be different for the sake of security.
Answer: B (LEAVE A REPLY)
With a Type 1 hypervisor, the management software and hardware are tightly tied together and provided by the same vendor on a closed platform. This allows for optimal security, performance, and support. The other answers are all incorrect descriptions of a Type 1 hypervisor.

NEW QUESTION: 2
Which of the following threat types can occur when an application does not properly validate input and can be leveraged to send users to malicious sites that appear to be legitimate?
A. Unvalidated redirects and forwards
B. Insecure direct object references
C. Security miscomfiguration
D. Sensitive data exposure
Answer: A (LEAVE A REPLY)
Many web applications offer redirect or forward pages that send users to different, external sites. If these pages are not properly secured and validated, attackers can use the application to forward users off to sites for phishing or malware attempts. These attempts can often be more successful than direct phishing attempts because users will trust the site or application that sent them there, and they will assume it has been properly validated and

approved by the trusted application's owners or operators. Security misconfiguration occurs when applications and systems are not properly configured for security--often a result of misapplied or inadequate baselines. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data.

NEW QUESTION: 3
If bit-splitting is used to store data sets across multiple jurisdictions, how may this enhance security?
Response:
A. By restricting privilege user access
B. By making seizure of data by law enforcement more difficult
C. By hiding it from attackers in a specific jurisdiction
D. By ensuring that users can only accidentally disclose data to one geographic area
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
Which protocol, as a part of TLS, handles negotiating and establishing a connection between two parties?
A. Record
B. Binding
C. Negotiation
D. Handshake
Answer: D (LEAVE A REPLY)
Explanation
The TLS handshake protocol is what negotiates and establishes the TLS connection between two parties and enables a secure communications channel to then handle data transmissions. The TLS record protocol is the actual secure communications method for transmitting data; it's responsible for the encryption and authentication of packets throughout their transmission between the parties, and in some cases it also performs compression. Negotiation and binding are not protocols under TLS.

NEW QUESTION: 5
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 (LEAVE A REPLY)

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: 6
With a federated identity system, where would a user perform their authentication when requesting services or application access?
A. Cloud provider
B. The application
C. Their home organization
D. Third-party authentication system
Answer: C (LEAVE A REPLY)
With a federated identity system, a user will perform authentication with their home organization, and the application will accept the authentication tokens and user information from the identity provider in order to grant access. The purpose of a federated system is to allow users to authenticate from their home organization. Therefore, using the application or a third-party authentication system would be contrary to the purpose of a federated system because it necessitates the creation of additional accounts. The use of a cloud provider would not be relevant to the operations of a federated system.

NEW QUESTION: 7
What are SOC 1/SOC 2/SOC 3?
A. Audit reports
B. Risk management frameworks
C. Access controls
D. Software developments
Answer: A (LEAVE A REPLY)
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: 8
What are SOCI/SOCII/SOCIII?
A. Software development phases
B. Risk management frameworks
C. Audit reports
D. Access controls

Answer: C (LEAVE A REPLY)

NEW QUESTION: 9
Tokenization requires at least ____ database(s).
A. Four
B. Three
C. One
D. Two
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10
What is the biggest negative to leasing space in a data center versus building or maintain your own?
A. Costs
B. Control
C. Certification
D. Regulation
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
When leasing space in a data center, an organization will give up a large degree of control as to how it is built and maintained, and instead must conform to the policies and procedures of the owners and operators of the data center.

NEW QUESTION: 11
How many additional DNS queries are needed when DNSSEC integrity checks are added?
A. Three
B. Zero
C. One
D. Two
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
DNSSEC does not require any additional DNS queries to be performed. The DNSSEC integrity checks and validations are all performed as part of the single DNS lookup resolution.

NEW QUESTION: 12
What must be secured on physical hardware to prevent unauthorized access to systems?
A. BIOS
B. SSH

C. RDP
D. ALOM
Answer: A (LEAVE A REPLY)
BIOS is the firmware that governs the physical initiation and boot up of a piece of hardware. If it is compromised, an attacker could have access to hosted systems and make configurations changes to expose or disable some security elements on the system.

NEW QUESTION: 13
Although indirect identifiers cannot alone point to an individual, the more of them known can lead to a specific identity. Which strategy can be used to avoid such a connection being made?
Response:
A. Obfuscation
B. Masking
C. Encryption
D. Anonymization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 14
Which of the following is NOT a component of access control?
A. Accounting
B. Federation
C. Authorization
D. Authentication
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Federation is not a component of access control. Instead, it is used to allow users possessing credentials from other authorities and systems to access services outside of their domain. This allows for access and trust without the need to create additional, local credentials. Access control encompasses not only the key concepts of authorization and authentication, but also accounting. Accounting consists of collecting and maintaining logs for both authentication and authorization for operational and regulatory requirements.

NEW QUESTION: 15
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: (SHOW ANSWER)
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: 16
Because PaaS implementations are so often used for software development, what is one of the vulnerabilities that should always be kept in mind?
A. Loss/theft of portable devices
B. Backdoors
C. DoS/DDoS
D. Malware
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
DAST checks software functionality in _____.
Response:
A. A runtime state
B. An IaaS configuration
C. The cloud
D. The production environment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
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 (LEAVE A REPLY)

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: 19
When an API is being leveraged, it will encapsulate its data for transmission back to the requesting party or service.
What is the data encapsulation used with the SOAP protocol referred to as?
A. Packet
B. Payload
C. Object
D. Envelope
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Simple Object Access Protocol (SOAP) encapsulates its information in what is known as a SOAP envelope. It then leverages common communications protocols for transmission. Object is a type of cloud storage, but also a commonly used term with certain types of programming languages. Packet and payload are terms that sound similar to envelope but are not correct in this case.

NEW QUESTION: 20
Which of the following is NOT a function performed by the handshake protocol of TLS?
A. Key exchange
B. Encryption
C. Negotiation of connection
D. Establish session ID
Answer: B (LEAVE A REPLY)
Explanation
The handshake protocol negotiates and establishes the connection as well as handles the key exchange and establishes the session ID. It does not perform the actual encryption of data packets.

NEW QUESTION: 21
When using an IaaS solution, what is a key benefit provided to the customer?
A. Metered and priced on the basis of units consumed
B. Increased energy and cooling system efficiencies
C. Transferred cost of ownership
D. The ability to scale up infrastructure services based on projected usage
Answer: A (LEAVE A REPLY)

IaaS has a number of key benefits for organizations, which include but are not limited to these: -- - Usage is metered and priced on the basis of units (or instances) consumed. This can also be billed back to specific departments or functions.
- It has an ability to scale up and down infrastructure services based on actual usage. This is particularly useful and beneficial where there are significant spikes and dips within the usage curve for infrastructure.
- It has a reduced cost of ownership. There is no need to buy assets for everyday use, no loss of asset value over time, and reduced costs of maintenance and support.
- It has a reduced energy and cooling costs along with "green IT" environment effect with optimum use of IT resources and systems.

NEW QUESTION: 22
When a data center is configured such that the backs of the devices face each other and the ambient temperature in the work area is cool, it is called _____.
Response:
A. Hot aisle containment
B. Cold aisle containment
C. Thermo-optimized
D. HVAC modulated
Answer: (SHOW ANSWER)

NEW QUESTION: 23
What are the four cloud deployment models?
A. External, Private, Hybrid, and Community
B. Public, Private, Joint, and Community
C. Public, Internal, Hybrid, and Community
D. Public, Private, Hybrid, and Community
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
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 (LEAVE A REPLY)
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: 25
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 (LEAVE A REPLY)
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: 26
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 (LEAVE A REPLY)
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: 27
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 (LEAVE A REPLY)
Explanation/Reference:
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: 28
Which of the following is a risk in the cloud environment that is not existing or is as prevalent in the legacy environment?
Response:
A. Loss of productivity due to DDoS
B. Ability of users to gain access to their physical workplace
C. Legal liability in multiple jurisdictions
D. Fire
Answer: (SHOW ANSWER)

NEW QUESTION: 29
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 (LEAVE A REPLY)
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: 30

_____ can often be the result of inadvertent activity.
Response:
A. Phishing
B. Disasters
C. Sprawl
D. DDoS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?
A. Infrastructure
B. Platform
C. Application
D. Data
Answer: D (LEAVE A REPLY)
Explanation
Regardless of which cloud-hosting model is used, the cloud customer always has sole responsibility for the data and its security.

NEW QUESTION: 32
What is the intellectual property protection for a useful manufacturing innovation?
A. Trademark
B. Copyright
C. patent
D. Trade secret
Answer: C (LEAVE A REPLY)
Patents protect processes (as well as inventions, new plantlife, and decorative patterns). The other answers listed are answers to other questions.

NEW QUESTION: 33

What is the first stage of the cloud data lifecycle where security controls can be implemented?

A. Use

B. Store

C. Share

D. Create

Answer: B (LEAVE A REPLY)

The "store" phase of the cloud data lifecycle, which typically occurs simultaneously with the "create" phase, or immediately thereafter, is the first phase where security controls can be implemented. In most case, the manner in which the data is stored will be based on its classification.

NEW QUESTION: 34

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

A. Active

B. Static

C. Dynamic

D. Transactional

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

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

NEW QUESTION: 35

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

A. Notification

B. Key identification

C. Data collection

D. Virtual image snapshots

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 36
Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like:
Response:
A. XSS and SQL injection
B. Syn floods
C. Password cracking
D. Ransomware
Answer: (SHOW ANSWER)

NEW QUESTION: 37
The Restatement (Second) Conflict of Law refers to which of the following?
Response:
A. Whether local or federal laws apply in a situation
B. The basis for deciding which laws are most appropriate in a situation where conflicting laws exist
C. When judges restate the law in an opinion
D. How jurisdictional disputes are settled
Answer: (SHOW ANSWER)

NEW QUESTION: 38
An organization could have many reasons that are common throughout the industry to activate a BCDR situation. Which of the following is NOT a typical reason to activate a BCDR plan?
A. Staff loss
B. Utility outage
C. Terrorist attack
D. Natural disaster
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the required amount of time to restore services to the predetermined level?
A. RPO
B. RSL
C. RTO
D. SRE
Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 40
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 (LEAVE A REPLY)
Explanation/Reference:
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: 41
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 (LEAVE A REPLY)
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: 42

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 (LEAVE A REPLY)
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: 43
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: (SHOW ANSWER)
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: 44
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 (LEAVE A REPLY)
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: 45
Which of the following roles is responsible for gathering metrics on cloud services and managing cloud deployments and the deployment processes?
A. Cloud service business manager
B. Cloud service operations manager
C. Cloud service manager
D. Cloud service deployment manager
Answer: (SHOW ANSWER)
The cloud service deployment manager is responsible for gathering metrics on cloud services, managing cloud deployments and the deployment process, and defining the environments and processes.

NEW QUESTION: 46
What type of solution is at the core of virtually all directory services?
A. WS
B. LDAP
C. ADFS
D. PKI
Answer: B (LEAVE A REPLY)
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: 47
The WS-Security standards are built around all of the following standards except which one?
A. SAML
B. WDSL

C. XML
D. SOAP
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The WS-Security specifications, as well as the WS-Federation system, are built upon XML, WDSL, and SOAP. SAML is a very similar protocol that is used as an alternative to WS.XML, WDSL, and SOAP are all integral to the WS-Security specifications.

NEW QUESTION: 48
What controls the formatting and security settings of a volume storage system within a cloud environment?
A. Management plane
B. SAN host controller
C. Hypervisor
D. Operating system of the host
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Once a storage LUN is allocated to a virtual machine, the operating system of that virtual machine will format, manage, and control the file system and security of the data on that LUN.

NEW QUESTION: 49
What are the U.S. Commerce Department controls on technology exports known as?
A. ITAR
B. DRM
C. EAR
D. EAL
Answer: (SHOW ANSWER)
EAR is a Commerce Department program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Digital rights management tools are used for protecting electronic processing of intellectual property.

NEW QUESTION: 50
Within an Infrastructure as a Service model, which of the following would NOT be a measured service?
A. CPU
B. Storage
C. Number of users
D. Memory

Answer: C (LEAVE A REPLY)
Explanation
Within IaaS, the number of users on a system is not relevant to the particular hosting model in regard to cloud resources. IaaS is focused on infrastructure needs of a system or application. Therefore, a factor such as the number of users that could affect licensing requirements, for example, would apply to the SaaS model, or in some instances to PaaS.

NEW QUESTION: 51
When an organization is considering a cloud environment for hosting BCDR solutions, which of the following would be the greatest concern?
A. Self-service
B. Resource pooling
C. Availability
D. Location
Answer: D (LEAVE A REPLY)
Explanation
If an organization wants to use a cloud service for BCDR, the location of the cloud hosting becomes a very important security consideration due to regulations and jurisdiction, which could be dramatically different from the organization's normal hosting locations. Availability is a hallmark of any cloud service provider, and likely will not be a prime consideration when an organization is considering using a cloud for BCDR; the same goes for self-service options. Resource pooling is common among all cloud systems and would not be a concern when an organization is dealing with the provisioning of resources during a disaster.

NEW QUESTION: 52
Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality?
A. Anonymization
B. Tokenization
C. Obfuscation
D. Masking
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
Vulnerability scans are dependent on _____ in order to function.
Response:
A. Malware libraries
B. Privileged access
C. Forensic analysis
D. Vulnerability signatures

Answer: (SHOW ANSWER)

NEW QUESTION: 54
Which of the following statements about Type 1 hypervisors is true?
A. The hardware vendor and software vendor are different.
B. The hardware vendor and software vendor are the same
C. The hardware vendor provides an open platform for software vendors.
D. The hardware vendor and software vendor should always be different for the sake of security.
Answer: B (LEAVE A REPLY)
Explanation
Explanation:
With a Type 1 hypervisor, the management software and hardware are tightly tied together and provided by the same vendor on a closed platform. This allows for optimal security, performance, and support. The other answers are all incorrect descriptions of a Type 1 hypervisor.

NEW QUESTION: 55
What type of redundancy can we expect to find in a datacenter of any tier?
Response:
A. Emergency egress
B. All infrastructure
C. Full power capabilities
D. All operational components
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
What is a serious complication an organization faces from the perspective of compliance with international operations?
A. Different certifications
B. Multiple jurisdictions
C. Different capabilities
D. Different operational procedures
Answer: B (LEAVE A REPLY)
When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, and many times they might be in contention with one other or not clearly applicable. These requirements can include the location of the users and the type of data they enter into systems, the laws governing the organization that owns the application and any regulatory requirements they may have, as well as the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which might be multiple jurisdictions as well.

NEW QUESTION: 57
Which of the following aspects of security is solely the responsibility of the cloud provider?
A. Regulatory compliance
B. Physical security
C. Operating system auditing
D. Personal security of developers
Answer: B (LEAVE A REPLY)
Regardless of the particular cloud service used, physical security of hardware and facilities is always the sole responsibility of the cloud provider. The cloud provider may release information about their physical security policies and procedures to ensure any particular requirements of potential customers will meet their regulatory obligations. Personal security of developers and regulatory compliance are always the responsibility of the cloud customer. Responsibility for operating systems, and the auditing of them, will differ based on the cloud service category used.

NEW QUESTION: 58
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 (LEAVE A REPLY)
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: 59
For service provisioning and support, what is the ideal amount of interaction between a cloud customer and cloud provider?
A. Half
B. Full
C. Minimal
D. Depends on the contract
Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 60
Which security concept would business continuity and disaster recovery fall under?
A. Confidentiality
B. Availability
C. Fault tolerance
D. Integrity
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Disaster recovery and business continuity are vital concerns with availability. If data is destroyed or compromised, having regular backup systems in place as well as being able to perform disaster recovery in the event of a major or widespread problem allows operations to continue with an acceptable loss of time and data to management. This also ensures that sensitive data is protected and persisted in the event of the loss or corruption of data systems or physical storage systems.

NEW QUESTION: 61
In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?
A. HIPAA
B. The contract
C. Statutes
D. Security control matrix
Answer: B (LEAVE A REPLY)
The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable.
The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

NEW QUESTION: 62
What are third-party providers of IAM functions for the cloud environment?
A. CASBs
B. DLPs
C. AESs
D. SIEMs
Answer: (SHOW ANSWER)

NEW QUESTION: 63
What's a potential problem when object storage versus volume storage is used within IaaS for application use and dependency?
A. Object storage is only optimized for small files.
B. Object storage is its own system, and data consistency depends on replication.
C. Object storage may have availability issues.
D. Object storage is dependent on access control from the host server.
Answer: B (LEAVE A REPLY)
Object storage runs on its own independent systems, which have their own redundancy and distribution. To ensure data consistency, sufficient time is needed for objects to fully replicate to all potential locations before being accessed. Object storage is optimized for high availability and will not be any less reliable than any other virtual machine within a cloud environment. It is hosted on a separate system that does not have dependencies in local host servers for access control, and it is optimized for files of all different sizes and uses.

NEW QUESTION: 64
Which of the following security measures done at the network layer in a traditional data center are also applicable to a cloud environment?
A. Dedicated switches
B. Trust zones
C. Redundant network circuits
D. Direct connections
Answer: (SHOW ANSWER)
Explanation/Reference:

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

NEW QUESTION: 65
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 (LEAVE A REPLY)
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: 66
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 (LEAVE A REPLY)
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: 67
Although performing BCDR tests at regular intervals is a best practice to ensure processes and documentation are still relevant and efficient, which of the following represents a reason to conduct a BCDR review outside of the regular interval?
Response:
A. Regulatory changes
B. Staff changes
C. Management changes
D. Application changes
Answer: D (LEAVE A REPLY)

NEW QUESTION: 68
When considering the option to migrate from an on-premises environment to a hosted cloud service, an organization should weigh the risks of allowing external entities to access the cloud data for collaborative purposes against _____.
Response:
A. Inviting external personnel into the legacy workspace in order to enhance collaboration
B. Disclosing the data publicly
C. Not securing the data in the legacy environment
D. Sending the data outside the legacy environment for collaborative purposes
Answer: (SHOW ANSWER)

NEW QUESTION: 69
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: (SHOW ANSWER)
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: 70
Impact resulting from risk being realized is often measured in terms of _____.
A. Amount of property lost
B. Number of people affected
C. Money
D. Amount of data lost
Answer: (SHOW ANSWER)

NEW QUESTION: 71
What is the first stage of the cloud data lifecycle where security controls can be implemented?
A. Use
B. Store
C. Share
D. Create
Answer: B (LEAVE A REPLY)
The "store" phase of the cloud data lifecycle, which typically occurs simultaneously with the "create" phase, or immediately thereafter, is the first phase where security controls can be

implemented. In most case, the manner in which the data is stored will be based on its classification.

NEW QUESTION: 72
Which of the following is NOT one of the cloud computing activities, as outlined in ISO/IEC 17789?
Response:
A. Cloud service administrator
B. Cloud service partner
C. Cloud service customer
D. Cloud service provider
Answer: A (LEAVE A REPLY)

NEW QUESTION: 73
When a customer performs a penetration test in the cloud, why isn't the test an optimum simu-lation of attack conditions?
Response:
A. When cloud customers use malware, it's not the same as when attackers use malware
B. Attackers don't use remote access for cloud activity
C. Advanced notice removes the element of surprise
D. Regulator involvement changes the attack surface
Answer: (SHOW ANSWER)

NEW QUESTION: 74
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 (LEAVE A REPLY)
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: 75
A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence.
Which core concept of cloud computing is most related to vendor lock-in?
A. Scalability
B. Interoperability
C. Portability

D. Reversibility

Answer: C (LEAVE A REPLY)

Explanation

Portability is the ability for a cloud customer to easily move their systems, services, and applications among different cloud providers. By avoiding reliance on proprietary APIs and other vendor-specific cloud features, an organization can maintain flexibility to move among the various cloud providers with greater ease.

Reversibility refers to the ability for a cloud customer to quickly and easy remove all their services and data from a cloud provider. Interoperability is the ability to reuse services and components for other applications and uses. Scalability refers to the ability of a cloud environment to add or remove resources to meet current demands.

NEW QUESTION: 76

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 (LEAVE A REPLY)

Explanation/Reference:

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: 77

If a cloud computing customer wishes to guarantee that a minimum level of resources will always be available, which of the following set of services would compromise the reservation?

A. Memory and networking

B. CPU and software

C. CPU and storage

D. CPU and memory

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources. A reservation pertains to memory and CPU resources. Under the concept of a reservation, memory and CPU are the guaranteed resources, but storage and networking are not included even though they are core components of cloud computing. Software would be out of scope for a guarantee and doesn't really pertain to the concept.

NEW QUESTION: 78

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

A. SRE

B. RTO

C. RPO

D. RSL

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 79

Which cloud service category is MOST likely to use a client-side key management system?

Response:

A. PaaS

B. DaaS

C. IaaS

D. SaaS

Answer: D (LEAVE A REPLY)

NEW QUESTION: 80

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

A. Sensitive data exposure

B. Security misconfiguration

C. Insecure direct object references

D. Unvalidated redirect and forwards

Answer: C (LEAVE A REPLY)

Explanation

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

Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner.

NEW QUESTION: 81

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

A. Extensive and comprehensive training programs, including initial, recurring, and refresher sessions

B. Skills and knowledge testing

C. Hardened perimeter devices

D. Aggressive background checks

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Hardened perimeter devices are more useful at attenuating the risk of external attack.

NEW QUESTION: 82

Which of the following is a restriction that can be enforced by information rights management (IRM) that is not possible for traditional file system controls?

A. Delete

B. Modify

C. Read

D. Print

Answer: D (LEAVE A REPLY)

Explanation
IRM allows an organization to control who can print a set of information. This is not be possible under traditional file system controls, where if a user can read a file, they are able to print it as well.

NEW QUESTION: 83
All of the following entitles are required to use FedRAMP-accredited Cloud Service Providers except
_____.
Response:
A. The CIA
B. The US post office
C. Federal Express
D. The Department of Homeland Security
Answer: C (LEAVE A REPLY)

NEW QUESTION: 84
Having a reservation in a cloud environment can ensure operations continue in the event of high utilization across the cloud.
Which of the following would NOT be a capability covered by reservations?
A. Performing business operations
B. Starting virtual machines
C. Running applications
D. Auto-scaling
Answer: D (LEAVE A REPLY)
Explanation
A reservation will not guarantee auto-scaling is available because it involves the allocation of additional resources beyond what a cloud customer already has provisioned.
Reservations will guarantee minimal resources are available to start virtual machines, run applications, and perform normal business operations.

NEW QUESTION: 85
Which data state would be most likely to use digital signatures as a security protection mechanism?
A. Data in use
B. Data in transit
C. Archived
D. Data at rest
Answer: A (LEAVE A REPLY)
Explanation

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

NEW QUESTION: 86
Which of the following roles involves overseeing billing, purchasing, and requesting audit reports for an organization within a cloud environment?
A. Cloud service user
B. Cloud service business manager
C. Cloud service administrator
D. Cloud service integrator
Answer: B (LEAVE A REPLY)
Explanation
The cloud service business manager is responsible for overseeing business and billing administration, purchasing cloud services, and requesting audit reports when necessary

NEW QUESTION: 87
Data labels could include all the following, except:
A. Distribution limitations
B. Multifactor authentication
C. Confidentiality level
D. Access restrictions
Answer: (SHOW ANSWER)
All the others might be included in data labels, but multifactor authentication is a procedure used for access control, not a label.

NEW QUESTION: 88
Which of the following concepts is NOT one of the core components to an encryption system architecture?
A. Software
B. Network
C. Keys
D. Data
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The network utilized is not one of the key components of an encryption system architecture. In fact, a network is not even required for encryption systems or the

processing and protection of data. The data, software used for the encryption engine itself, and the keys used to implement the encryption are all core components of an encryption system architecture.

NEW QUESTION: 89
Which of the following best describes the Organizational Normative Framework (ONF)?
A. A set of application security, and best practices, catalogued and leveraged by the organization
B. A container for components of an application's security, best practices catalogued and leveraged by the organization
C. A framework of containers for some of the components of application security, best practices, catalogued and leveraged by the organization
D. A framework of containers for all components of application security, best practices, catalogued and leveraged by the organization.
Answer: D (LEAVE A REPLY)
Explanation
Option B is incorrect, because it refers to a specific applications security elements, meaning it is about an ANF, not the ONF. C is true, but not as complete as D, making D the better choice. C suggests that the framework contains only "some" of the components, which is why B (which describes "all" components) is better

NEW QUESTION: 90
Which of the following threat types involves an application developer leaving references to internal information and configurations in code that is exposed to the client?
A. Sensitive data exposure
B. Security misconfiguration
C. Insecure direct object references
D. Unvalidated redirect and forwards
Answer: C (LEAVE A REPLY)
An insecure direct object reference occurs when a developer has in their code a reference to something on the application side, such as a database key, the directory structure of the application, configuration information about the hosting system, or any other information that pertains to the workings of the application that should not be exposed to users or the network.
Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, allowing spoofing for malware of phishing attacks.
Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data. Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner.

NEW QUESTION: 91
Which of the following is the dominant driver behind the regulations to which a system or application must adhere?
A. Data source
B. Locality
C. Contract
D. SLA
Answer: (SHOW ANSWER)
The locality--or physical location and jurisdiction where the system or data resides--is the dominant driver of regulations. This may be based on the type of data contained within the application or the way in which the data is used. The contract and SLA both articulate requirements for regulatory compliance and the responsibilities for the cloud provider and cloud customer, but neither artifact defines the actual requirements. Instead, the contract and SLA merely form the official documentation between the cloud provider and cloud customer. The source of the data may place contractual requirements or best practice guidelines on its usage, but ultimately jurisdiction has legal force and greater authority.

NEW QUESTION: 92
Which of the following roles involves testing, monitoring, and securing cloud services for an organization?
A. Cloud service integrator
B. Cloud service business manager
C. Cloud service user
D. Cloud service administrator
Answer: D (LEAVE A REPLY)
Explanation
The cloud service administrator is responsible for testing cloud services, monitoring services, administering security for services, providing usage reports on cloud services, and addressing problem reports

NEW QUESTION: 93

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

A. Personnel data

B. Security profiles

C. Publications

D. Financial records

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 94

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 (LEAVE A REPLY)

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: 95

Gap analysis is performed for what reason?

A. To begin the benchmarking process

B. To assure proper accounting practices are being used

C. To provide assurances to cloud customers

D. To ensure all controls are in place and working properly

Answer: (SHOW ANSWER)

The primary purpose of the gap analysis is to begin the benchmarking process against risk and security standards and frameworks.

NEW QUESTION: 96

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 (LEAVE A REPLY)
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: 97
What type of security threat is DNSSEC designed to prevent?
A. Account hijacking
B. Snooping
C. Spoofing
D. Injection
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
DNSSEC is designed to prevent the spoofing and redirection of DNS resolutions to rogue sites.

NEW QUESTION: 98
You work for a government research facility. Your organization often shares data with other government research organizations.
You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations.
Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.
If you don't use cross-certification, what other model can you implement for this purpose?
A. Mandatory access control (MAC)
B. Cloud reseller
C. Intractable nuanced variance
D. Third-party identity broker
Answer: D (LEAVE A REPLY)

NEW QUESTION: 99
The goals of DLP solution implementation include all of the following, except:
A. Elasticity
B. Policy enforcement
C. Data discovery

D. Loss of mitigation

Answer: A (LEAVE A REPLY)

Explanation

DLP does not have anything to do with elasticity, which is the capability of the environment to scale up or down according to demand. All the rest are goals of DLP implementations.

NEW QUESTION: 100

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

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

A. IDS

B. IPS

C. Proxy

D. Firewall

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

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

NEW QUESTION: 101

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 (LEAVE A REPLY)

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: 102
Which of the following are the storage types associated with IaaS?
A. Object and target
B. Volume and container
C. Volume and label
D. Volume and object
Answer: D (LEAVE A REPLY)

NEW QUESTION: 103
Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?
Response:
A. Mapping to existing access control lists (ACLs)
B. Delineating biometric catalogs
C. Preventing multifactor authentication
D. Prohibiting unauthorized transposition
Answer: A (LEAVE A REPLY)

NEW QUESTION: 104
Which of the following roles is responsible for overseeing customer relationships and the processing of financial transactions?
A. Cloud service manager
B. Cloud service deployment
C. Cloud service business manager
D. Cloud service operations manager
Answer: C (LEAVE A REPLY)
The cloud service business manager is responsible for overseeing business plans and customer relationships as well as processing financial transactions.

NEW QUESTION: 105
Which type of controls are the SOC Type 1 reports specifically focused on?
A. Integrity
B. PII
C. Financial
D. Privacy
Answer: (SHOW ANSWER)
Explanation
SOC Type 1 reports are focused specifically on internal controls as they relate to financial reporting.

NEW QUESTION: 106

What controls the formatting and security settings of a volume storage system within a cloud environment?

A. Management plane

B. SAN host controller

C. Hypervisor

D. Operating system of the host

Answer: D (LEAVE A REPLY)

Once a storage LUN is allocated to a virtual machine, the operating system of that virtual machine will format, manage, and control the file system and security of the data on that LUN.

NEW QUESTION: 107

Which of the following is the recommended operating range for temperature and humidity in a data center?

A. Between 60 °F - 85 °F and 40% and 60% relative humidity

B. Between 64 °F - 81 °F and 40% and 60% relative humidity

C. Between 62 °F - 81 °F and 40% and 65% relative humidity

D. Between 64 °F - 84 °F and 30% and 60% relative humidity

Answer: B (LEAVE A REPLY)

NEW QUESTION: 108

What is used with a single sign-on system for authentication after the identity provider has successfully authenticated a user?

A. SAML

B. Token

C. Key

D. XML

Answer: (SHOW ANSWER)

NEW QUESTION: 109

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

A. SOC 1 Type 1
B. SOC 2 Type 2
C. SOC 3
D. SOC 1 Type 2
Answer: C (LEAVE A REPLY)
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: 110
The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program has
_____ tiers.
A. Two
B. Three
C. Four
D. Eight
Answer: (SHOW ANSWER)

NEW QUESTION: 111
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: (SHOW ANSWER)
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: 112
With an application hosted in a cloud environment, who could be the recipient of an eDiscovery order?
A. Users
B. Both the cloud provider and cloud customer
C. The cloud customer
D. The cloud provider
Answer: B (LEAVE A REPLY)
Explanation

Either the cloud customer or the cloud provider could receive an eDiscovery order, and in almost all circumstances they would need to work together to ensure compliance.

NEW QUESTION: 113
Which network protocol is essential for allowing automation and orchestration within a cloud environment?
Response:
A. DNSSEC
B. VLANs
C. IPsec
D. DHCP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 114
What aspect of data center planning occurs first?
A. Physical design
B. Audit
C. Policy revision
D. Logical design
Answer: A (LEAVE A REPLY)

NEW QUESTION: 115
Which of the following is a restriction that can be enforced by information rights management (IRM) that is not possible for traditional file system controls?
A. Delete
B. Modify
C. Read
D. Print
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
IRM allows an organization to control who can print a set of information. This is not be possible under traditional file system controls, where if a user can read a file, they are able to print it as well.

NEW QUESTION: 116
What masking strategy involves the replacing of sensitive data at the time it is accessed and used as it flows between the data and application layers of a service?
A. Active
B. Static
C. Dynamic

D. Transactional

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 117

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 (LEAVE A REPLY)

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: 118

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

A. REST and SAML

B. SOAP and REST

C. REST and XML

D. XML and SAML

Answer: B (LEAVE A REPLY)

Explanation

Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) are the most commonly used APIs within a cloud environment. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data.

NEW QUESTION: 119

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

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

NEW QUESTION: 120
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 (LEAVE A REPLY)
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: 121
Which of the cloud deployment models offers the easiest initial setup and access for the cloud customer?
A. Hybrid
B. Community
C. Private
D. Public
Answer: (SHOW ANSWER)
Because the public cloud model is available to everyone, in most instances all a customer will need to do to gain access is set up an account and provide a credit card number through the service's web portal. No additional contract negotiations, agreements, or specific group memberships are typically needed to get started.

NEW QUESTION: 122
The European Union is often considered the world leader in regard to the privacy of personal data and has declared privacy to be a "human right." In what year did the EU first assert this principle?
A. 1995
B. 2000
C. 2010
D. 1999
Answer: A (LEAVE A REPLY)
Explanation
The EU passed Directive 95/46 EC in 1995, which established data privacy as a human right. The other years listed are incorrect.

NEW QUESTION: 123
Which of the following is the least challenging with regard to eDiscovery in the cloud?
A. Identifying roles such as data owner, controller and processor
B. Decentralization of data storage
C. Forensic analysis
D. Complexities of International law
Answer: C (LEAVE A REPLY)
Forensic analysis is the least challenging of the answers provided as it refers to the analysis of data once it is obtained. The challenges revolve around obtaining the data for analysis due to the complexities of international law, the decentralization of data storage or difficulty knowing where to look, and identifying the data owner, controller, and processor.

NEW QUESTION: 124
Which type of cloud-based storage is IRM typically associated with?
Response:
A. Unstructured
B. Volume
C. Structured

D. Object
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Which process serves to prove the identity and credentials of a user requesting access to an application or data?
A. Repudiation
B. Authentication
C. Identification
D. Authorization
Answer: B (LEAVE A REPLY)
Authentication is the process of proving whether the identity presented by a user is true and valid. This can be done through common mechanisms such as user ID and password combinations or with more secure methods such as multifactor authentication.

NEW QUESTION: 126
Which of the following pertains to a macro level approach to data center design rather than the traditional tiered approach to data centers?
A. IDCA
B. NFPA
C. BICSI
D. Uptime Institute
Answer: A (LEAVE A REPLY)
The standards put out by the International Data Center Authority (IDCA) have established the Infinity Paradigm, which is intended to be a comprehensive data center design and operations framework. The Infinity Paradigm shifts away from many models that rely on tiered architecture for data centers, where each successive tier increases redundancy. Instead, it emphasizes data centers being approached at a macro level, without a specific and isolated focus on certain aspects to achieve tier status.

NEW QUESTION: 127
Which SSAE 16 audit report is simply an attestation of audit results?
Response:
A. SOC 2, Type 2
B. SOC 3
C. SOC 1
D. SOC 2, Type 1
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Which of the following statements accurately describes VLANs?

A. They are not restricted to the same data center or the same racks.
B. They are not restricted to the name rack but restricted to the same data center.
C. They are restricted to the same racks and data centers.
D. They are not restricted to the same rack but restricted to same switches.
Answer: A (LEAVE A REPLY)
A virtual area network (VLAN) can span any networks within a data center, or it can span across different physical locations and data centers.

NEW QUESTION: 129
Which of the following is the optimal temperature for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?
A. 69.8-86.0degF (21-30degC)
B. 64.4-80.6degF(18-27degC)
C. 51.8-66.2degF(11-19degC)
D. 44.6-60-8degF(7-16degC)
Answer: B (LEAVE A REPLY)
The guidelines from ASHRAE establish 64.4-80.6degF (18-27degC) as the optimal temperature for a data center.

NEW QUESTION: 130
Impact resulting from risk being realized is often measured in terms of _____.
A. Amount of data lost
B. Money
C. Amount of property lost
D. Number of people affected
Answer: B (LEAVE A REPLY)

NEW QUESTION: 131
Your company has just been served with an eDiscovery order to collect event data and other pertinent information from your application during a specific period of time, to be used as potential evidence for a court proceeding.
Which of the following, apart from ensuring that you collect all pertinent data, would be the MOST important consideration?
Response:
A. Confidentiality
B. Chain of custody
C. Encryption
D. Compression
Answer: B (LEAVE A REPLY)

NEW QUESTION: 132
Which component of ITIL involves the creation of an RFC ticket and obtaining official approvals for it?
A. Problem management
B. Release management
C. Deployment management
D. Change management
Answer: D (LEAVE A REPLY)
The change management process involves the creation of the official Request for Change (RFC) ticket, which is used to document the change, obtain the required approvals from management and stakeholders, and track the change to completion. Release management is a subcomponent of change management, where the actual code or configuration change is put into place. Deployment management is similar to release management, but it's where changes are actually implemented on systems. Problem management is focused on the identification and mitigation of known problems and deficiencies before they are able to occur.

NEW QUESTION: 133
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: (SHOW ANSWER)
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: 134
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: (SHOW ANSWER)
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: 135
Which of the following is a valid risk management metric?
A. KPI
B. KRI
C. SOC
D. SLA
Answer: B (LEAVE A REPLY)
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: 136
A honeypot should contain _____ data.
A. Raw
B. Useless
C. Production
D. Sensitive
Answer: B (LEAVE A REPLY)

NEW QUESTION: 137
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 (LEAVE A REPLY)
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: 138
Which of the following represents a control on the maximum amount of resources that a single customer, virtual machine, or application can consume within a cloud environment?
A. Share
B. Reservation
C. Provision
D. Limit
Answer: D (LEAVE A REPLY)
Limits are put in place to enforce a maximum on the amount of memory or processing a cloud customer can use. This can be done either on a virtual machine or as a comprehensive whole for a customer, and is meant to ensure that enormous cloud resources cannot be allocated or consumed by a single host or customer to the detriment of other hosts and customers.

NEW QUESTION: 139
Data transformation in a cloud environment should be of great concern to organizations considering cloud migration because _____ could affect data classification processes/implementations.
Response:
A. Multitenancy
B. Remote access
C. Physical distance
D. Virtualization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140

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 (LEAVE A REPLY)
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: 141
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 (LEAVE A REPLY)
Conflict of interest is a threat, not a control.

NEW QUESTION: 142
Which of the following practices can enhance both operational capabilities and configuration management efforts?
Response:
A. Regular backups
B. Constant uptime
C. File hashes
D. Multifactor authentication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
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: (SHOW ANSWER)
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: 144
What aspect of data center planning occurs first?
Response:
A. Policy revision
B. Logical design
C. Audit
D. Physical design
Answer: D (LEAVE A REPLY)

NEW QUESTION: 145
Which of the following cloud aspects complicates eDiscovery?
A. Resource pooling
B. On-demand self-service
C. Multitenancy
D. Measured service
Answer: C (LEAVE A REPLY)
With multitenancy, eDiscovery becomes more complicated because the data collection involves extra steps to ensure that only those customers or systems that are within scope are turned over to the requesting authority.

NEW QUESTION: 146
Which of the following roles would be responsible for managing memberships in federations and the use and integration of federated services?
A. Inter-cloud provider
B. Cloud service business manager
C. Cloud service administrator
D. Cloud service integrator
Answer: A (LEAVE A REPLY)
The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated services. A cloud service administrator is responsible for testing, monitoring, and securing cloud services, as well as providing usage reporting and dealing with service problems. The cloud service integrator is responsible for connecting existing systems and services with a cloud. The cloud service

business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

NEW QUESTION: 147
Which of the following does NOT fall under the "IT" aspect of quality of service (QoS)?
A. Applications
B. Key performance indicators (KPIs)
C. Services
D. Security
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
KPIs fall under the "business" aspect of QoS, along with monitoring and measuring of events and business processes. Services, security, and applications are all core components and concepts of the "IT" aspect of QoS.

NEW QUESTION: 148
You are the security director for a chain of automotive repair centers across several states. Your company uses a cloud SaaS provider, for business functions that cross several of the locations of your facilities, such as: 1) ordering parts 2) logistics and inventory 3) billing, and 4) marketing.
The manager at one of your newest locations reports that there is a competing car repair company that has a logo that looks almost exactly like the one your company uses. What will most likely affect the determination of who has ownership of the logo?
Response:
A. The jurisdiction where both businesses are using the logo simultaneously
B. Whichever entity has the most customers that recognize the logo
C. Whoever first used the logo
D. Whoever first applied for legal protection of the logo
Answer: (SHOW ANSWER)

NEW QUESTION: 149
What are SOC 1/SOC 2/SOC 3?
A. Audit reports
B. Risk management frameworks
C. Access controls
D. Software developments
Answer: A (LEAVE A REPLY)
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: 150
Which of the following terms is NOT a commonly used category of risk acceptance?
A. Moderate
B. Critical
C. Minimal
D. Accepted
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation
Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

NEW QUESTION: 151
You are the IT security manager for a video game software development company. Which of the following is most likely to be your primary concern on a daily basis?
A. Security flaws in your organization
B. Regulatory compliance
C. Security flaws in your products
D. Health and human safety
Answer: A (LEAVE A REPLY)

NEW QUESTION: 152
Within a federated identity system, which of the following would you be MOST likely to use for sending information for consumption by a relying party?
A. XML
B. HTML
C. WS-Federation

D. SAML

Answer: (SHOW ANSWER)

The Security Assertion Markup Language (SAML) is the most widely used method for encoding and sending attributes and other information from an identity provider to a relying party.WS- Federation, which is used by Active Directory Federation Services (ADFS), is the second most used method for sending information to a relying party, but it is not a better choice than SAML.

XML is similar to SAML in the way it encodes and labels data, but it does not have all of the required extensions that SAML does. HTML is not used within federated systems at all.

NEW QUESTION: 153

Proper _____ need to be assigned to each data classification/category.

Response:

A. Dollar values

B. Policies

C. Metadata

D. Security controls

Answer: D (LEAVE A REPLY)

NEW QUESTION: 154

Which of the following is the optimal humidity level for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?

A. 30-50 percent relative humidity

B. 50-75 percent relative humidity

C. 20-40 percent relative humidity

D. 40-60 percent relative humidity

Answer: D (LEAVE A REPLY)

The guidelines from ASHRAE establish 40-60 percent relative humidity as optimal for a data center.

NEW QUESTION: 155

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 (LEAVE A REPLY)

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: 156
In the cloud motif, the data owner is usually:
A. The cloud provider
B. In another jurisdiction
C. The cloud customer
D. The cloud access security broker
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The data owner is usually considered the cloud customer in a cloud configuration; the data in question is the customer's information, being processed in the cloud. The cloud provider is only leasing services and hardware to the customer. The cloud access security broker (CASB) only handles access control on behalf of the cloud customer, and is not in direct contact with the production data.

NEW QUESTION: 157
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:
A. Tokenization
B. Masking
C. Data discovery
D. Obfuscation
Answer: C (LEAVE A REPLY)
Data discovery is a term used to describe the process of identifying information according to specific traits or categories. The rest are all methods for obscuring data.

NEW QUESTION: 158
If a cloud computing customer wishes to guarantee that a minimum level of resources will always be available, which of the following set of services would compromise the reservation?
A. Memory and networking
B. CPU and software
C. CPU and storage
D. CPU and memory

Answer: D (LEAVE A REPLY)
A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources. A reservation pertains to memory and CPU resources. Under the concept of a reservation, memory and CPU are the guaranteed resources, but storage and networking are not included even though they are core components of cloud computing. Software would be out of scope for a guarantee and doesn't really pertain to the concept.

NEW QUESTION: 159
When an organization is considering the use of cloud services for BCDR planning and solutions, which of the following cloud concepts would be the most important?
A. Reversibility
B. Elasticity
C. Interoperability
D. Portability
Answer: D (LEAVE A REPLY)
Portability is the ability for a service or system to easily move among different cloud providers.
This is essential for using a cloud solution for BCDR because vendor lock-in would inhibit easily moving and setting up services in the event of a disaster, or it would necessitate a large number of configuration or component changes to implement. Interoperability, or the ability to reuse components for other services or systems, would not be an important factor for BCDR.
Reversibility, or the ability to remove all data quickly and completely from a cloud environment, would be important at the end of a disaster, but would not be important during setup and deployment. Elasticity, or the ability to resize resources to meet current demand, would be very beneficial to a BCDR situation, but not as vital as portability.

NEW QUESTION: 160
Which of the following storage types are used with an Infrastructure as a Service (IaaS) solution?
Response:
A. Unstructured and ephemeral
B. Volume and object
C. Volume and block
D. Structured and object
Answer: (SHOW ANSWER)

NEW QUESTION: 161
Who is the entity identified by personal data?

Response:
A. The data custodian
B. The data processor
C. The data subject
D. The data owner
Answer: C (LEAVE A REPLY)

NEW QUESTION: 162
What is a key capability or characteristic of PaaS?
A. Support for a homogenous environment
B. Support for a single programming language
C. Ability to reduce lock-in
D. Ability to manually scale
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
PaaS should have the following key capabilities and characteristics:
- Support multiple languages and frameworks: PaaS should support multiple programming languages and frameworks, thus enabling the developers to code in whichever language they prefer or the design requirements specify. In recent times, significant strides and efforts have been taken to ensure that open source stacks are both supported and utilized, thus reducing "lock-in" or issues with interoperability when changing CSPs.
- Multiple hosting environments: The ability to support a wide variety of underlying hosting environments for the platform is key to meeting customer requirements and demands. Whether public cloud, private cloud, local hypervisor, or bare metal, supporting multiple hosting environments allows the application developer or administrator to migrate the application when and as required. This can also be used as a form of contingency and continuity and to ensure the ongoing availability.
- Flexibility: Traditionally, platform providers provided features and requirements that they felt suited the client requirements, along with what suited their service offering and positioned them as the provider of choice, with limited options for the customers to move easily. This has changed drastically, with extensibility and flexibility now afforded to meeting the needs and requirements of developer audiences.
This has been heavily influenced by open source, which allows relevant plug-ins to be quickly and efficiently introduced into the platform.
- Allow choice and reduce lock-in: PaaS learns from previous horror stories and restrictions, proprietary meant red tape, barriers, and restrictions on what developers could do when it came to migration or adding features and components to the platform. Although the requirement to code to specific APIs was made available by the providers, they could run their apps in various environments based on commonality and standard API structures, ensuring a level of consistency and quality for customers and users.

- Ability to auto-scale: This enables the application to seamlessly scale up and down as required to accommodate the cyclical demands of users. The platform will allocate resources and assign these to the application as required. This serves as a key driver for any seasonal organizations that experience spikes and drops in usage.

NEW QUESTION: 163
Although performing BCDR tests at regular intervals is a best practice to ensure processes and documentation are still relevant and efficient, which of the following represents a reason to conduct a BCDR review outside of the regular interval?
A. Regulatory changes
B. Application changes
C. Staff changes
D. Management changes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 164
DLP solutions can aid in deterring loss due to which of the following?
A. Inadvertent disclosure
B. Natural disaster
C. Randomization
D. Device failure
Answer: A (LEAVE A REPLY)
Explanation/Reference:
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: 165
Which of the following is a management role, versus a technical role, as it pertains to data management and oversight?
A. Data owner
B. Data processor
C. Database administrator
D. Data custodian
Answer: A (LEAVE A REPLY)
Data owner is a management role that's responsible for all aspects of how data is used and protected. The database administrator, data custodian, and data processor are all technical roles that involve the actual use and consumption of data, or the implementation of security controls and policies with the data.

NEW QUESTION: 166
What type of storage structure does object storage employ to maintain files?
A. Directory
B. Hierarchical
C. tree
D. Flat
Answer: (SHOW ANSWER)
Object storage uses a flat file system to hold storage objects; it assigns files a key value that is then used to access them, rather than relying on directories or descriptive filenames. Typical storage layouts such as tree, directory, and hierarchical structures are used within volume storage, whereas object storage maintains a flat structure with key values.

NEW QUESTION: 167
In the cloud motif, the data owner is usually:
A. The cloud provider
B. In another jurisdiction
C. The cloud customer
D. The cloud access security broker
Answer: C (LEAVE A REPLY)
The data owner is usually considered the cloud customer in a cloud configuration; the data in question is the customer's information, being processed in the cloud. The cloud provider is only leasing services and hardware to the customer. The cloud access security broker (CASB) only handles access control on behalf of the cloud customer, and is not in direct contact with the production data.

NEW QUESTION: 168
When an API is being leveraged, it will encapsulate its data for transmission back to the requesting party or service.
What is the data encapsulation used with the SOAP protocol referred to as?
A. Packet
B. Payload

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

NEW QUESTION: 169
Which of the following is not a way to manage risk?
A. Enveloping
B. Accepting
C. Transferring
D. Mitigating
Answer: A (LEAVE A REPLY)

NEW QUESTION: 170
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 (LEAVE A REPLY)
Explanation/Reference:
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: 171
The physical layout of a cloud data center campus should include redundancies of all the following except
_____.
Response:
A. Communications connectivity lines
B. Physical perimeter security controls (fences, lights, walls, etc.)
C. The administration/support staff building
D. Electrical utility lines
Answer: C (LEAVE A REPLY)

NEW QUESTION: 172
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 (LEAVE A REPLY)
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: 173
The cloud customer's trust in the cloud provider can be enhanced by all of the following except:
A. SLAs
B. Shared administration
C. Audits
D. real-time video surveillance
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Video surveillance will not provide meaningful information and will not enhance trust. All the others will do it.

NEW QUESTION: 174
In a cloud environment, encryption should be used for all the following, except:
A. Secure sessions/VPN
B. Long-term storage of data
C. Near-term storage of virtualized images
D. Profile formatting
Answer: D (LEAVE A REPLY)
All of these activities should incorporate encryption, except for profile formatting, which is a made-up term.

NEW QUESTION: 175
Which data sanitation method is also commonly referred to as "zeroing"?

A. Overwriting
B. Nullification
C. Blanking
D. Deleting
Answer: (SHOW ANSWER)
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: 176
All of the following are usually nonfunctional requirements except _____.
A. Function
B. Color
C. Security
D. Sound
Answer: A (LEAVE A REPLY)

NEW QUESTION: 177
What is a serious complication an organization faces from the compliance perspective with international operations?
A. Multiple jurisdictions
B. Different certifications
C. Different operational procedures
D. Different capabilities
Answer: A (LEAVE A REPLY)
Explanation
When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, which often may not be clearly applicable or may be in contention with each other. These requirements can involve the location of the users and the type of data they enter into systems, the laws governing the organization that owns the application and any regulatory requirements they may have, and finally the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which may be multiple jurisdictions as well. Different certifications would not come into play as a challenge because the major IT and data center certifications are international and would apply to any cloud provider. Different capabilities and different operational procedures would be mitigated by the organization's selection of a cloud provider and would not be a challenge if an appropriate provider was chosen, regardless of location.

NEW QUESTION: 178

Why might an organization choose to comply with the ISO 27001 standard?
Response:
A. Price
B. International acceptance
C. Speed
D. Ease of implementation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 179
Different security testing methodologies offer different strategies and approaches to testing systems, requiring security personnel to determine the best type to use for their specific circumstances.
What does dynamic application security testing (DAST) NOT entail that SAST does?
A. Discovery
B. Knowledge of the system
C. Scanning
D. Probing
Answer: B (LEAVE A REPLY)
Explanation
Dynamic application security testing (DAST) is considered "black-box" testing and begins with no inside knowledge of the application or its configurations. Everything about it must be discovered during its testing.
As with most types of testing, dynamic application security testing (DAST) involves probing, scanning, and a discovery process for system information.

NEW QUESTION: 180
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: (SHOW ANSWER)
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: 181
What is the best approach for dealing with services or utilities that are installed on a system but not needed to perform their desired function?
A. Remove

B. Monitor
C. Disable
D. Stop
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The best practice is to totally remove any unneeded services and utilities on a system to prevent any chance of compromise or use. If they are just disabled, it is possible for them to be inadvertently started again at any point, or another exploit could be used to start them again. Removing also negates the need to patch and maintain them going forward.

NEW QUESTION: 182
In application-level encryption, where does the encryption engine reside?
A. Within the database accessed by the application
B. In the OS on which the application is run
C. In the application accessing the database
D. In the volume where the database resides
Answer: C (LEAVE A REPLY)

NEW QUESTION: 183
What does nonrepudiation mean?
Response:
A. Preventing any party that participates in a transaction from claiming that it did not
B. Ensuring that someone cannot turn off auditing capabilities while performing a function
C. Ensuring that a transaction is completed before saving the results
D. Prohibiting certain parties from a private conversation
Answer: (SHOW ANSWER)

NEW QUESTION: 184
Which of the following is NOT a factor that is part of a firewall configuration?
A. Encryption
B. Port

C. Protocol
D. Source IP
Answer: A (LEAVE A REPLY)
Firewalls take into account source IP, destination IP, the port the traffic is using, as well as the network protocol (UDP/TCP). Whether or not the traffic is encrypted is not something a firewall is concerned with.

NEW QUESTION: 185
Which security concept would business continuity and disaster recovery fall under?
A. Confidentiality
B. Availability
C. Fault tolerance
D. Integrity
Answer: B (LEAVE A REPLY)
Disaster recovery and business continuity are vital concerns with availability. If data is destroyed or compromised, having regular backup systems in place as well as being able to perform disaster recovery in the event of a major or widespread problem allows operations to continue with an acceptable loss of time and data to management. This also ensures that sensitive data is protected and persisted in the event of the loss or corruption of data systems or physical storage systems.

NEW QUESTION: 186
Which of the following is the least challenging with regard to eDiscovery in the cloud?
A. Identifying roles such as data owner, controller and processor
B. Decentralization of data storage
C. Forensic analysis
D. Complexities of International law
Answer: C (LEAVE A REPLY)
Explanation
Forensic analysis is the least challenging of the answers provided as it refers to the analysis of data once it is obtained. The challenges revolve around obtaining the data for analysis due to the complexities of international law, the decentralization of data storage or difficulty knowing where to look, and identifying the data owner, controller, and processor.

NEW QUESTION: 187
Which of the following terms is not associated with cloud forensics?
A. eDiscovery
B. Chain of custody
C. Analysis
D. Plausibility
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 188
What sort of legal enforcement may the Payment Card Industry (PCI) Security Standards Council not bring to bear against organizations that fail to comply with the Payment Card Industry Data Security Standard (PCI DSS)?
Response:
A. Subject to increased audit frequency and scope
B. Suspension of credit card processing privileges
C. Fines
D. Jail time
Answer: D (LEAVE A REPLY)

NEW QUESTION: 189
What is the data encapsulation used with the SOAP protocol referred to?
A. Packet
B. Envelope
C. Payload
D. Object
Answer: B (LEAVE A REPLY)
Explanation
Simple Object Access Protocol (SOAP) encapsulates its information in what is known as a SOAP envelope and then leverages common communications protocols for transmission.

NEW QUESTION: 190
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 (LEAVE A REPLY)
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: 191

Which cloud service category brings with it the most expensive startup costs, but also the lowest costs for ongoing support and maintenance staff?
A. SaaS
B. DaaS
C. PaaS
D. IaaS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 192
What aspect of a Type 2 hypervisor involves additional security concerns that are not relevant with a Type 1 hypervisor?
Response:
A. Programming languages
B. Reliance on a host operating system
C. Auditing
D. Proprietary software
Answer: B (LEAVE A REPLY)

NEW QUESTION: 193
What expectation of data custodians is made much more challenging by a cloud implementation, especially with PaaS or SaaS?
A. Data classification
B. Knowledge of systems
C. Access to data
D. Encryption requirements
Answer: B (LEAVE A REPLY)
Explanation
Under the Federal Rules of Civil Procedure, data custodians are assumed and expected to have full and comprehensive knowledge of the internal design and architecture of their systems. In a cloud environment, especially with PaaS and SaaS, it is impossible for the data custodian to have this knowledge because those systems are controlled by the cloud provider and protected as proprietary knowledge.

NEW QUESTION: 194
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing.
According to the CSA, what aspect of managed cloud services makes the threat of malicious insiders so alarming?
A. Multitenancy
B. Scalability
C. Flexibility

D. Metered service
Answer: A (LEAVE A REPLY)

NEW QUESTION: 195
Which security concept is focused on the trustworthiness of data?
A. Integrity
B. Availability
C. Nonrepudiation
D. Confidentiality
Answer: (SHOW ANSWER)
Integrity is focused on the trustworthiness of data as well as the prevention of unauthorized modification or tampering of it. A prime consideration for maintaining integrity is an emphasis on the change management and configuration management aspects of operations, so that all modifications are predictable, tracked, logged, and verified, whether they are performed by actual human users or systems processes and scripts.

NEW QUESTION: 196
When an organization implements an SIEM solution and begins aggregating event data, the configured event sources are only valid at the time it was configured.
Application modifications, patching, and other upgrades will change the events generated and how they are represented over time.
What process is necessary to ensure events are collected and processed with this in mind?
A. Aggregation updates
B. Continual review
C. Continuous optimization
D. Event elasticity
Answer: C (LEAVE A REPLY)

NEW QUESTION: 197
Which of the following would probably best aid an organization in deciding whether to migrate from a legacy environment to a particular cloud provider?

Response:
A. SLA satisfaction surveys from other (current and past) cloud customers
B. The cost/benefit measure of closing the organization's relocation site (hot site/warm site) and using the cloud for disaster recovery instead
C. Cloud provider offers to provide engineering assistance during the migration
D. Rate sheets comparing a cloud provider to other cloud providers
Answer: (SHOW ANSWER)

NEW QUESTION: 198
Which of the following would NOT be considered part of resource pooling with an Infrastructure as a Service implementation?
A. Storage
B. Application
C. Mamory
D. CPU
Answer: B (LEAVE A REPLY)
Explanation
Infrastructure as a Service pools the compute resources for platforms and applications to build upon, including CPU, memory, and storage. Applications are not part of an IaaS offering from the cloud provider.

NEW QUESTION: 199
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 (LEAVE A REPLY)
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: 200
If a company needed to guarantee through contract and SLAs that a cloud provider would always have available sufficient resources to start their services and provide a certain level of provisioning, what would the contract need to refer to?
A. Limit
B. Reservation

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

NEW QUESTION: 201
In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?
A. HIPAA
B. The contract
C. Statutes
D. Security control matrix
Answer: B (LEAVE A REPLY)
The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable. The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

NEW QUESTION: 202
What type of solution is at the core of virtually all directory services?
A. WS
B. LDAP
C. ADFS
D. PKI
Answer: B (LEAVE A REPLY)
Explanation/Reference:
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: 203
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 (LEAVE A REPLY)
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: 204
Which of the following publishes the most commonly used standard for data center design in regard to tiers and topologies?
A. IDCA
B. Uptime Institute
C. NFPA
D. BICSI
Answer: (SHOW ANSWER)
Explanation
The Uptime Institute publishes the most commonly used and widely known standard on data center tiers and topologies. It is based on a series of four tiers, with each progressive increase in number representing more stringent, reliable, and redundant systems for security, connectivity, fault tolerance, redundancy, and cooling.

NEW QUESTION: 205
In order to prevent cloud customers from potentially consuming enormous amounts of resources within a cloud environment and thus having a negative impact on other customers, what concept is commonly used by a cloud provider?
A. Limit
B. Cap
C. Throttle
D. Reservation

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

NEW QUESTION: 206
Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?
A. Data
B. Personnel
C. Cash
D. Systems
Answer: C (LEAVE A REPLY)

NEW QUESTION: 207
The European Union is often considered the world leader in regard to the privacy of personal data and has declared privacy to be a "human right." In what year did the EU first assert this principle?
A. 1995
B. 2000
C. 2010
D. 1999
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The EU passed Directive 95/46 EC in 1995, which established data privacy as a human right. The other years listed are incorrect.

NEW QUESTION: 208
The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet). In a typical TLS session, what is the usual means for establishing trust between the parties?
A. Out-of-band authentication
B. PKI certificates
C. Multifactor authentication

D. Preexisting knowledge of each other
Answer: B (LEAVE A REPLY)

NEW QUESTION: 209
Which is the appropriate phase of the cloud data lifecycle for determining the data's classification?
A. Create
B. Use
C. Share
D. Store
Answer: A (LEAVE A REPLY)
Explanation
Explanation:
Any time data is created, modified, or imported, the classification needs to be evaluated and set from the earliest phase to ensure security is always properly maintained for the duration of its lifecycle.

NEW QUESTION: 210
Which data sanitation method is also commonly referred to as "zeroing"?
A. Overwriting
B. Nullification
C. Blanking
D. Deleting
Answer: A (LEAVE A REPLY)
Explanation/Reference:
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: 211
What concept does the "T" represent in the STRIDE threat model?
A. TLS
B. Testing
C. Tampering with data
D. Transport
Answer: C (LEAVE A REPLY)
Explanation
Explanation
Any application that sends data to the user will face the potential that the user could manipulate or alter the data, whether it resides in cookies, GET or POST commands, or

headers, or manipulates client-side validations. If the user receives data from the application, it is crucial that the application validate and verify any data that is received back from the user.

NEW QUESTION: 212
Which cloud deployment model is MOST likely to offer free or very cheap services to users?
A. Hybrid
B. Community
C. Public
D. Private
Answer: C (LEAVE A REPLY)
Public clouds offer services to anyone, regardless of affiliation, and are the most likely to offer free services to users. Examples of public clouds with free services include iCloud, Dropbox, and OneDrive.
Private cloud models are designed for specific customers and for their needs, and would not offer services to the public at large, for free or otherwise. A community cloud is specific to a group of similar organizations and would not offer free or widely available public services. A hybrid cloud model would not fit the specifics of the question.

NEW QUESTION: 213
Which type of software is most likely to be reviewed by the most personnel, with the most varied perspectives?
A. Open source software
B. Database management software
C. Secure software
D. Proprietary software
Answer: A (LEAVE A REPLY)

NEW QUESTION: 214
Which of the following is a possible negative aspect of bit-splitting?
A. Loss of public image

B. Greater chance of physical theft of assets
C. A small fire hazard
D. Some risk to availability, depending on the implementation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 215
An audit against the _____ will demonstrate that an organization has a holistic, comprehensive security program.
Response:
A. ISO 27001 certification requirements
B. SAS 70 standard
C. SOC 2, Type 2 report matrix
D. SSAE 16 standard
Answer: (SHOW ANSWER)

NEW QUESTION: 216
Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?
A. Six months
B. One month
C. One year
D. One week
Answer: (SHOW ANSWER)
SOC Type 2 reports are focused on the same policies and procedures, as well as their effectiveness, as SOC Type 1 reports, but are evaluated over a period of at least six consecutive months, rather than a finite point in time.

NEW QUESTION: 217
When using a SaaS solution, what is the capability provided to the customer?
A. To use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
B. To use the consumer's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers,

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

NEW QUESTION: 218
Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.
Which of the following is NOT a regulatory system from the United States federal government?
A. HIPAA
B. SOX
C. FISMA
D. PCI DSS
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The Payment Card Industry Data Security Standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry-regulatory standard, not a governmental one. The Sarbanes-Oxley Act (SOX) was passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders. The Health Insurance Portability and Accountability Act (HIPAA) was

passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

NEW QUESTION: 219
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the required amount of time to restore services to the predetermined level?
A. RPO
B. RSL
C. RTO
D. SRE
Answer: C (LEAVE A REPLY)
Explanation
The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the predetermined level of operations necessary during a BCDR situation. SRE is provided as an erroneous response.

NEW QUESTION: 220
In which cloud service model is the customer required to maintain the OS?
A. Iaas
B. CaaS
C. PaaS
D. SaaS
Answer: A (LEAVE A REPLY)
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: 221
Fiber-optic lines are considered part of layer _____ of the OSI model.
Response:
A. 1
B. 7
C. 5
D. 3
Answer: A (LEAVE A REPLY)

NEW QUESTION: 222
The management plane is used to administer a cloud environment and perform administrative tasks across a variety of systems, but most specifically it's used with the hypervisors.
What does the management plane typically leverage for this orchestration?
A. APIs
B. Scripts
C. TLS
D. XML
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The management plane uses APIs to execute remote calls across the cloud environment to various management systems, especially hypervisors. This allows a centralized administrative interface, often a web portal, to orchestrate tasks throughout an enterprise. Scripts may be utilized to execute API calls, but they are not used directly to interact with systems. XML is used for data encoding and transmission, but not for executing remote calls. TLS is used to encrypt communications and may be used with API calls, but it is not the actual process for executing commands.

NEW QUESTION: 223
From the perspective of compliance, what is the most important consideration when it comes to data center location?
A. Natural disasters
B. Utility access
C. Jurisdiction
D. Personnel access
Answer: (SHOW ANSWER)
Jurisdiction will dictate much of the compliance and audit requirements for a data center. Although all the aspects listed are very important to security, from a strict compliance perspective, jurisdiction is the most important. Personnel access, natural disasters, and utility access are all important operational considerations for selecting a data center location, but they are not related to compliance issues like jurisdiction is.

NEW QUESTION: 224
Which of the following standards primarily pertains to cabling designs and setups in a data center?
A. IDCA
B. BICSI
C. NFPA

D. Uptime Institute

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 225

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

A. Relying party

B. Service originator

C. Service relay

D. Service relay

Answer: A (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 226

What is a key component of GLBA?

Response:

A. The right to audit

B. The right to be forgotten

C. EU Data Directives

D. The information security program

Answer: D (LEAVE A REPLY)

NEW QUESTION: 227

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 (LEAVE A REPLY)
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: 228
Why are PaaS environments at a higher likelihood of suffering backdoor vulnerabilities?
A. They are often used for software development.
B. They rely on virtualization.
C. They are scalable.
D. They have multitenancy.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 229
Every security program and process should have which of the following?
A. Severe penalties
B. Multifactor authentication
C. Foundational policy
D. Homomorphic encryption
Answer: (SHOW ANSWER)
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: 230
What concept does the "T" represent in the STRIDE threat model?

A. TLS
B. Testing
C. Tampering with data
D. Transport
Answer: C (LEAVE A REPLY)
Explanation
Any application that sends data to the user will face the potential that the user could manipulate or alter the data, whether it resides in cookies, GET or POST commands, or headers, or manipulates client-side validations. If the user receives data from the application, it is crucial that the application validate and verify any data that is received back from the user.

NEW QUESTION: 231
Which Common Criteria Evaluation Assurance Level (EAL) is granted to those products that are formally verified in terms of design and tested by an independent third party?
A. 3
B. 5
C. 7
D. 1
Answer: C (LEAVE A REPLY)

NEW QUESTION: 232
How is an object stored within an object storage system?
A. Key value
B. Database
C. LDAP
D. Tree structure
Answer: (SHOW ANSWER)
Explanation
Object storage uses a flat structure with key values to store and access objects.

NEW QUESTION: 233
You need to gain approval to begin moving your company's data and systems into a cloud environment.
However, your CEO has mandated the ability to easily remove your IT assets from the cloud provider as a precondition.
Which of the following cloud concepts would this pertain to?
A. Removability
B. Extraction
C. Portability
D. Reversibility

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

NEW QUESTION: 234
Which of the following is a widely used tool for code development, branching, and collaboration?
A. GitHub
B. Maestro
C. Orchestrator
D. Conductor
Answer: (SHOW ANSWER)
Explanation
GitHub is an open source tool that developers leverage for code collaboration, branching, and versioning.

NEW QUESTION: 235
What type of security threat is DNSSEC designed to prevent?
A. Account hijacking
B. Snooping
C. Spoofing
D. Injection
Answer: (SHOW ANSWER)
DNSSEC is designed to prevent the spoofing and redirection of DNS resolutions to rogue sites.

NEW QUESTION: 236
To protect data on user devices in a BYOD environment, the organization should consider requiring all the following, except:
A. Multifactor authentication
B. DLP agents
C. Two-person integrity
D. Local encryption
Answer: (SHOW ANSWER)
Although all the other options are ways to harden a mobile device, two-person integrity is a concept that has nothing to do with the topic, and, if implemented, would require everyone in your organization to walk around in pairs while using their mobile devices.

NEW QUESTION: 237
You work for a government research facility. Your organization often shares data with other government research organizations.
You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations.
Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.
In order to pass the user IDs and authenticating credentials of each user among the organizations, what protocol/language/motif will you most likely utilize?
Response:
A. Simple Object Access Protocol (SOAP)
B. Security Assertion Markup Language (SAML)
C. Representational State Transfer (REST)
D. Hypertext Markup Language (HTML)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 238
Without the extensive funds of a large corporation, a small-sized company could gain considerable and cost-effective services for which of the following concepts by moving to a cloud environment?
A. Regulatory
B. Security
C. Testing
D. Development
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Cloud environments, regardless of the specific deployment model used, have extensive and robust security controls in place, especially in regard to physical and infrastructure security. A small company can leverage the extensive security controls and monitoring provided by a cloud provider, which they would unlikely ever be able to afford on their own.
Moving to a cloud would not result in any gains for development and testing because these areas require the same rigor regardless of where deployment and hosting occur.
Regulatory compliance in a cloud would not be a gain for an organization because it would likely result in additional oversight and auditing as well as require the organization to adapt to a new environment.

NEW QUESTION: 239

What is the primary security mechanism used to protect SOAP and REST APIs?
A. Firewalls
B. WAFs
C. XML firewalls
D. Encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 240
Which data formats are most commonly used with the REST API?
A. JSON and SAML
B. XML and SAML
C. XML and JSON
D. SAML and HTML
Answer: (SHOW ANSWER)
JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API, and are typically implemented with caching for increased scalability and performance.

NEW QUESTION: 241
Which of the following is NOT one of the official risk rating categories?
A. Critical
B. Low
C. Catastrophic
D. Minimal
Answer: (SHOW ANSWER)
The official categories of cloud risk ratings are Minimal, Low, Moderate, High, and Critical.

NEW QUESTION: 242
When using an IaaS solution, what is a key benefit provided to the customer?
A. Metered and priced on the basis of units consumed
B. Increased energy and cooling system efficiencies
C. Transferred cost of ownership

D. The ability to scale up infrastructure services based on projected usage
Answer: (SHOW ANSWER)
IaaS has a number of key benefits for organizations, which include but are not limited to these: --
- Usage is metered and priced on the basis of units (or instances) consumed. This can also be billed back to specific departments or functions.
- It has an ability to scale up and down infrastructure services based on actual usage. This is particularly useful and beneficial where there are significant spikes and dips within the usage curve for infrastructure.
- It has a reduced cost of ownership. There is no need to buy assets for everyday use, no loss of asset value over time, and reduced costs of maintenance and support.
- It has a reduced energy and cooling costs along with "green IT" environment effect with optimum use of IT resources and systems.

NEW QUESTION: 243
What is the primary security mechanism used to protect SOAP and REST APIs?
Response:
A. XML firewalls
B. Encryption
C. WAFs
D. Firewalls
Answer: B (LEAVE A REPLY)

NEW QUESTION: 244
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: (SHOW ANSWER)
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: 245
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 (LEAVE A REPLY)
Explanation/Reference:
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: 246
Which of the following is not a security concern related to archiving data for long-term storage?
Response:
A. Format of the data
B. Media the data resides on
C. Long-term storage of the related cryptographic keys
D. Underground depth of the storage facility
Answer: D (LEAVE A REPLY)

NEW QUESTION: 247
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 (LEAVE A REPLY)
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: 248
Which of the following practices can enhance both operational capabilities and configuration management efforts?
A. Constant uptime
B. File hashes
C. Regular backups
D. Multifactor authentication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 249
What must SOAP rely on for security since it does not provide security as a built-in capability?
A. Encryption
B. Tokenization
C. TLS
D. SSL
Answer: A (LEAVE A REPLY)
Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for data passing, and it must rely on the encryption of those data packages for security. TLS and SSL (before it was deprecated) represent two commons approaches to using encryption for protection of data transmissions. However, they are only two possible options and do not encapsulate the overall concept the question is looking for.
Tokenization, which involves the replacement of sensitive data with opaque values, would not be appropriate for use with SOAP because the actual data is needed by the services.

NEW QUESTION: 250
Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.
Which of the following is NOT a regulatory system from the United States federal government?
A. HIPAA
B. SOX
C. FISMA
D. PCI DSS
Answer: (SHOW ANSWER)
Explanation
The Payment Card Industry Data Security Standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry-regulatory standard, not a governmental one. The Sarbanes-Oxley Act (SOX) was passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders. The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

NEW QUESTION: 251
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: (SHOW ANSWER)
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: 252
Which of the following is a risk in the cloud environment that is not existing or is as prevalent in the legacy environment?
A. Loss of productivity due to DDoS
B. Ability of users to gain access to their physical workplace
C. Fire
D. Legal liability in multiple jurisdictions
Answer: D (LEAVE A REPLY)

NEW QUESTION: 253
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: (SHOW ANSWER)
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: 254

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 (LEAVE A REPLY)
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: 255
What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?
A. Proxy
B. Bastion
C. Honeypot
D. WAF
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A bastion host is a server that is fully exposed to the public Internet, but is extremely hardened to prevent attacks and is usually dedicated for a specific application or usage; it is not something that will serve multiple purposes. This singular focus allows for much more stringent security hardening and monitoring.

NEW QUESTION: 256
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: (SHOW ANSWER)
Explanation/Reference:
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: 257
Which of the following pertains to a macro level approach to data center design rather than the traditional tiered approach to data centers?
A. IDCA
B. NFPA
C. BICSI
D. Uptime Institute
Answer: A (LEAVE A REPLY)
Explanation
The standards put out by the International Data Center Authority (IDCA) have established the Infinity Paradigm, which is intended to be a comprehensive data center design and operations framework. The Infinity Paradigm shifts away from many models that rely on tiered architecture for data centers, where each successive tier increases redundancy. Instead, it emphasizes data centers being approached at a macro level, without a specific and isolated focus on certain aspects to achieve tier status.

NEW QUESTION: 258
SOC 2 reports were intended to be _____.
Response:
A. Retained for internal use
B. Nonbinding
C. Released to the public
D. Only technical assessments
Answer: A (LEAVE A REPLY)

NEW QUESTION: 259
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 (LEAVE A REPLY)
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: 260
Which of the following pertains to fire safety standards within a data center, specifically with their enormous electrical consumption?
A. NFPA
B. BICSI
C. IDCA
D. Uptime Institute
Answer: (SHOW ANSWER)
The standards put out by the National Fire Protection Association (NFPA) cover general fire protection best practices for any type of facility, but also specific publications pertaining to IT equipment and data centers.

NEW QUESTION: 261
Which of the following is NOT a criterion for data within the scope of eDiscovery?
A. Possession
B. Custody
C. Control
D. Archive
Answer: D (LEAVE A REPLY)
eDiscovery pertains to information and data that is in the possession, control, and custody of an organization.

NEW QUESTION: 262
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 (LEAVE A REPLY)
Explanation
Mandatory breach reporting is the best example of regulated PII components. The rest are generally considered components of contractual PII.

NEW QUESTION: 263
Digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM) often protect unauthorized distribution of what type of intellectual property?
Response:
A. Patents
B. Personally identifiable information (PII)
C. Copyright
D. Trademarks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 264
Which of the following is a valid risk management metric?
A. KPI
B. KRI
C. SOC
D. SLA
Answer: B (LEAVE A REPLY)
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: 265
Which of the following is NOT a major regulatory framework?
A. PCI DSS
B. HIPAA
C. SOX
D. FIPS 140-2
Answer: D (LEAVE A REPLY)
FIPS 140-2 is a United States certification standard for cryptographic modules, and it provides guidance and requirements for their use based on the requirements of the data

classification. However, these are not actual regulatory requirements. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS) are all major regulatory frameworks either by law or specific to an industry.

NEW QUESTION: 266
What category of PII data can carry potential fines or even criminal charges for its improper use or disclosure?
A. Protected
B. Legal
C. Regulated
D. Contractual
Answer: (SHOW ANSWER)
Explanation
Regulated PII data carries legal and jurisdictional requirements, along with official penalties for its misuse or disclosure, which can be either civil or criminal in nature. Legal and protected are similar terms, but neither is the correct answer in this case. Contractual requirements can carry financial or contractual impacts for the improper use or disclosure of PII data, but not legal or criminal penalties that are officially enforced.

NEW QUESTION: 267
Which regulatory system pertains to the protection of healthcare data?
A. HIPAA
B. HAS
C. HITECH
D. HFCA
Answer: A (LEAVE A REPLY)
Explanation
The Health Insurance Portability and Accountability Act (HIPAA) sets stringent requirements in the United States for the protection of healthcare records.

NEW QUESTION: 268
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: (SHOW ANSWER)
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: 269
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 (LEAVE A REPLY)
Explanation/Reference:
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: 270
Your company operates in a highly competitive market, with extremely high-value data assets.
Senior management wants to migrate to a cloud environment but is concerned that providers will not meet the company's security needs.
Which deployment model would probably best suit the company's needs?
Response:
A. Community
B. Hybrid
C. Public
D. Private
Answer: D (LEAVE A REPLY)

NEW QUESTION: 271
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: (SHOW ANSWER)
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: 272
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months.
The 2013 OWASP Top Ten list includes "cross- site scripting (XSS)."
Which of the following is not a method for reducing the risk of XSS attacks?
A. XML escape all identity assertions.
B. Sanitize HTML markup with a library designed for the purpose.
C. Use an auto-escaping template system.
D. HTML escape JSON values in an HTML context and read the data with JSON.parse.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 273
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: (SHOW ANSWER)
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: 274
Which of the following service categories entails the least amount of support needed on the part of the cloud customer?
A. SaaS
B. IaaS
C. DaaS
D. PaaS
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
With SaaS providing a fully functioning application that is managed and maintained by the cloud provider, cloud customers incur the least amount of support responsibilities themselves of any service category.

NEW QUESTION: 275
Which of the following is not a component of contractual PII?
A. Scope of processing
B. Value of data
C. Location of data
D. Use of subcontractors
Answer: C (LEAVE A REPLY)
Explanation
The value of data itself has nothing to do with it being considered a part of contractual

NEW QUESTION: 276
With software-defined networking (SDN), which two types of network operations are segregated to allow for granularity and delegation of administrative access and functions?
A. Filtering and forwarding
B. Filtering and firewalling
C. Firewalling and forwarding
D. Forwarding and protocol

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

NEW QUESTION: 277
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 (LEAVE A REPLY)
Explanation
All the elements except adjudication need to be addressed in each policy. Adjudication is not an element of policy.

NEW QUESTION: 278
Which aspect of cloud computing makes it very difficult to perform repeat audits over time to track changes and compliance?
A. Virtualization
B. Multitenancy
C. Resource pooling
D. Dynamic optimization
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Cloud environments will regularly change virtual machines as patching and versions are changed. Unlike a physical environment, there is little continuity from one period of time to another. It is very unlikely that the same virtual machines would be in use during a repeat audit.

NEW QUESTION: 279
You are the security manager for a small application development company. Your company is considering the use of the cloud for software testing purposes. Which cloud service model is most likely to suit your needs?
A. PaaS
B. IaaS

C. SaaS
D. LaaS
Answer: (SHOW ANSWER)

NEW QUESTION: 280
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: (SHOW ANSWER)
Resource pooling serves as the biggest challenge to using DLP solutions to protect data at rest because data is spread across large systems, which are also shared by many different clients.
With the data always moving and being distributed, additional challenges for protection are created versus a physical and isolated storage system. Portability is the ability to easily move between different cloud providers, and interoperability is focused on the ability to reuse components or services. Reversibility pertains to the ability of a cloud customer to easily and completely remove their data and services from a cloud provider.

NEW QUESTION: 281
Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.
Which of the following is NOT a regulatory system from the United States federal government?
A. HIPAA
B. SOX
C. FISMA
D. PCI DSS
Answer: D (LEAVE A REPLY)
The Payment Card Industry Data Security Standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry-regulatory standard, not a governmental one.
The Sarbanes-Oxley Act (SOX) was passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders.
The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

NEW QUESTION: 282
What concept does the "T" represent in the STRIDE threat model?
A. TLS
B. Testing
C. Tampering with data
D. Transport
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation
Any application that sends data to the user will face the potential that the user could manipulate or alter the data, whether it resides in cookies, GET or POST commands, or headers, or manipulates client-side validations. If the user receives data from the application, it is crucial that the application validate and verify any data that is received back from the user.

NEW QUESTION: 283
Which of the following does NOT fall under the "IT" aspect of quality of service (QoS)?
A. Applications
B. Key performance indicators (KPIs)
C. Services
D. Security
Answer: (SHOW ANSWER)
KPIs fall under the "business" aspect of QoS, along with monitoring and measuring of events and business processes. Services, security, and applications are all core components and concepts of the "IT" aspect of QoS.

NEW QUESTION: 284
Which of the following in a federated environment is responsible for consuming authentication tokens?
A. Authentication provider
B. Relying party
C. Identity provider
D. Cloud services broker
Answer: B (LEAVE A REPLY)

NEW QUESTION: 285
All the following are data analytics modes, except:
A. Datamining
B. Agile business intelligence
C. Refractory iterations
D. Real-time analytics

Answer: C (LEAVE A REPLY)
All the others are data analytics methods, but "refractory iterations" is a nonsense term thrown in as a red herring.

NEW QUESTION: 286
What does the REST API use to protect data transmissions?
A. NetBIOS
B. VPN
C. Encapsulation
D. TLS
Answer: D (LEAVE A REPLY)
Explanation
Representational State Transfer (REST) uses TLS for communication over secured channels. Although REST also supports SSL, at this point SSL has been phased out due to vulnerabilities and has been replaced by TLS.

NEW QUESTION: 287
Which of the following features is a main benefit of PaaS over IaaS?
A. Location independence
B. High-availability
C. Physical security requirements
D. Auto-scaling
Answer: D (LEAVE A REPLY)
With PaaS providing a fully configured and managed framework, auto-scaling can be implemented to programmatically adjust resources based on the current demands of the environment.

NEW QUESTION: 288
What does a cloud customer purchase or obtain from a cloud provider?
A. Services
B. Hosting
C. Servers

D. Customers

Answer: (SHOW ANSWER)

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

NEW QUESTION: 289

Jurisdictions have a broad range of privacy requirements pertaining to the handling of personal data and information.

Which jurisdiction requires all storage and processing of data that pertains to its citizens to be done on hardware that is physically located within its borders?

A. Japan

B. United States

C. European Union

D. Russia

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The Russian government requires all data and processing of information about its citizens to be done solely on systems and applications that reside within the physical borders of the country. The United States, European Union, and Japan focus their data privacy laws on requirements and methods for the protection of data, rather than where the data physically resides.

NEW QUESTION: 290

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

A. Dependence on keys

B. Cipher strength

C. Efficiency

D. Protocol standards

Answer: A (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 291

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 (LEAVE A REPLY)

Explanation/Reference:

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: 292

Which of the following is NOT a factor that is part of a firewall configuration?

A. Encryption

B. Port

C. Protocol

D. Source IP

Answer: (SHOW ANSWER)

Explanation

Firewalls take into account source IP, destination IP, the port the traffic is using, as well as the network protocol (UDP/TCP). Whether or not the traffic is encrypted is not something a firewall is concerned with.

NEW QUESTION: 293

Modern web service systems are designed for high availability and resiliency. Which concept pertains to the ability to detect problems within a system, environment, or application and programmatically invoke redundant systems or processes for mitigation?

A. Elasticity

B. Redundancy

C. Fault tolerance

D. Automation

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Fault tolerance allows a system to continue functioning, even with degraded performance, if portions of it fail or degrade, without the entire system or service being taken down. It can detect problems within a service and invoke compensating systems or functions to keep functionality going. Although redundancy is similar to fault tolerance, it is more focused on having additional copies of systems available, either active or passive, that can take up services if one system goes down. Elasticity pertains to the ability of a system to resize to meet demands, but it is not focused on system failures. Automation, and its role in maintaining large systems with minimal intervention, is not directly related to fault tolerance.

NEW QUESTION: 294
Which technology can be useful during the "share" phase of the cloud data lifecycle to continue to protect data as it leaves the original system and security controls?
A. IPS
B. WAF
C. DLP
D. IDS
Answer: C (LEAVE A REPLY)
Data loss prevention (DLP) can be applied to data that is leaving the security enclave to continue to enforce access restrictions and policies on other clients and systems.

NEW QUESTION: 295
Which crucial aspect of cloud computing can be most threatened by insecure APIs?
A. Automation
B. Resource pooling
C. Elasticity
D. Redundancy
Answer: (SHOW ANSWER)
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: 296
_____ is the most prevalent protocol used in identity federation.
A. SAML
B. FTP
C. WS-Federation
D. HTTP

Answer: A (LEAVE A REPLY)

NEW QUESTION: 297
A federated identity system is composed of three main components. Which of the following is NOT one of the three main components?
A. Relying party
B. API
C. User
D. Identity provider
Answer: (SHOW ANSWER)

NEW QUESTION: 298
Having a reservation in a cloud environment can ensure operations continue in the event of high utilization across the cloud.
Which of the following would NOT be a capability covered by reservations?
A. Performing business operations
B. Starting virtual machines
C. Running applications
D. Auto-scaling
Answer: (SHOW ANSWER)
A reservation will not guarantee auto-scaling is available because it involves the allocation of additional resources beyond what a cloud customer already has provisioned.
Reservations will guarantee minimal resources are available to start virtual machines, run applications, and perform normal business operations.

NEW QUESTION: 299
Typically, SSDs are _____.
Response:
A. Larger than tape backup
B. More expensive than spinning platters
C. More subject to malware than legacy drives
D. Heavier than tape libraries
Answer: B (LEAVE A REPLY)

NEW QUESTION: 300
You are in charge of creating the BCDR plan and procedures for your organization. Your organization has its production environment hosted by a cloud provider, and you have appropriate protections in place.
Which of the following is a significant consideration for your BCDR backup?
Response:
A. Good cryptographic key management

B. Enough personnel at the BCDR recovery site to ensure proper operations
C. Access to the servers where the BCDR backup is stored
D. Forensic analysis capabilities
Answer: A (LEAVE A REPLY)

NEW QUESTION: 301
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 (LEAVE A REPLY)
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: 302

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

A. Data in use

B. Data in transit

C. Archived

D. Data at rest

Answer: (SHOW ANSWER)

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

NEW QUESTION: 303

Which ITIL component is focused on anticipating predictable problems and ensuring that configurations and operations are in place to prevent these problems from ever occurring?

A. Availability management

B. Continuity management

C. Configuration management

D. Problem management

Answer: D (LEAVE A REPLY)

Problem management is focused on identifying and mitigating known problems and deficiencies before they are able to occur, as well as on minimizing the impact of incidents that cannot be prevented.

Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster.

Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements.

Configuration management tracks and maintains detailed information about all IT components within an organization.

NEW QUESTION: 304

Tokenization requires at least ____ database(s).

Response:

A. Two

B. Three

C. Four

D. One

Answer: A (LEAVE A REPLY)

NEW QUESTION: 305
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 (LEAVE A REPLY)
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: 306
Which of the following is a method for apportioning resources that involves prioritizing resource requests to resolve contention situations?
Response:
A. Cancellations
B. Reservations
C. Shares
D. Limits
Answer: C (LEAVE A REPLY)

NEW QUESTION: 307
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 (LEAVE A REPLY)
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: 308
All policies within the organization should include a section that includes all of the following, except:
A. Policy adjudication
B. Policy enforcement
C. Policy maintenance
D. Policy review
Answer: A (LEAVE A REPLY)

NEW QUESTION: 309
Audits are either done based on the status of a system or application at a specific time or done as a study over a period of time that takes into account changes and processes. Which of the following pairs matches an audit type that is done over time, along with the minimum span of time necessary for it?
A. SOC Type 2, one year
B. SOC Type 1, one year
C. SOC Type 2, one month
D. SOC Type 2, six months
Answer: D (LEAVE A REPLY)
Explanation
SOC Type 2 audits are done over a period of time, with six months being the minimum duration. SOC Type 1 audits are designed with a scope that's a static point in time, and the other times provided for SOC Type 2 are incorrect.

NEW QUESTION: 310
What is a cloud storage architecture that manages the data in a hierarchy of files?
A. File-based storage
B. CDN
C. Object-based storage
D. Database
Answer: (SHOW ANSWER)

NEW QUESTION: 311
Which type of audit report is considered a "restricted use" report for its intended audience?

A. SAS-70
B. SSAE-16
C. SOC Type 1
D. SOC Type 2
Answer: (SHOW ANSWER)
Explanation
SOC Type 1 reports are considered "restricted use" reports. They are intended for management and stakeholders of an organization, clients of the service organization, and auditors of the organization. They are not intended for release beyond those audiences.

NEW QUESTION: 312
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 (LEAVE A REPLY)
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: 313
All of the following are identity federation standards commonly found in use today except _____.
Response:
A. OpenID
B. OAuth
C. WS-Federation
D. PGP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 314
Which of the following data sanitation methods would be the MOST effective if you needed to securely remove data as quickly as possible in a cloud environment?
A. Degaussing
B. Cryptographic erasure
C. Zeroing
D. Overwriting
Answer: (SHOW ANSWER)

NEW QUESTION: 315

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 (LEAVE A REPLY)
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: 316
Which type of audit report is considered a "restricted use" report for its intended audience?
A. SAS-70
B. SSAE-16
C. SOC Type 1
D. SOC Type 2
Answer: C (LEAVE A REPLY)
SOC Type 1 reports are considered "restricted use" reports. They are intended for management and stakeholders of an organization, clients of the service organization, and auditors of the organization. They are not intended for release beyond those audiences.

NEW QUESTION: 317
Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?
Response:
A. SOC 1
B. SOC 3
C. SOC 2
D. SOC 4
Answer: (SHOW ANSWER)

NEW QUESTION: 318
Each of the following is an element of the Identification phase of the identity and access management (IAM) process except _____.
Response:
A. Inversion
B. Management
C. Provisioning
D. Deprovisioning
Answer: (SHOW ANSWER)

NEW QUESTION: 319
What type of masking strategy involves making a separate and distinct copy of data with masking in place?
A. Dynamic
B. Replication
C. Static
D. Duplication
Answer: (SHOW ANSWER)
Explanation
With static masking, a separate and distinct copy of the data set is created with masking in place. This is typically done through a script or other process that takes a standard data set, processes it to mask the appropriate and predefined fields, and then outputs the data set as a new one with the completed masking done.

NEW QUESTION: 320
Which of the following roles is responsible for preparing systems for the cloud, administering and monitoring services, and managing inventory and assets?
A. Cloud service business manager
B. Cloud service deployment manager
C. Cloud service operations manager
D. Cloud service manager

Answer: C (LEAVE A REPLY)
The cloud service operations manager is responsible for preparing systems for the cloud, administering and monitoring services, providing audit data as requested or required, and managing inventory and assets.

NEW QUESTION: 321
What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?
A. Proxy
B. Bastion
C. Honeypot
D. WAF
Answer: B (LEAVE A REPLY)
A bastion host is a server that is fully exposed to the public Internet, but is extremely hardened to prevent attacks and is usually dedicated for a specific application or usage; it is not something that will serve multiple purposes. This singular focus allows for much more stringent security hardening and monitoring.

NEW QUESTION: 322
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 (LEAVE A REPLY)
Explanation
Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe. The rest are not.

NEW QUESTION: 323
For optimal security, trust zones are used for network segmentation and isolation. They allow for the separation of various systems and tiers, each with its own security level. Which of the following is typically used to allow administrative personnel access to trust zones?
A. IPSec
B. SSH
C. VPN
D. TLS
Answer: C (LEAVE A REPLY)
Explanation

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

NEW QUESTION: 324
You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center. One of the challenges you're facing is whether the provider will have undue control over your data once it is within the provider's data center; will the provider be able to hold your organization hostage because they have your data?
This is a(n) _____ issue.
A. Portability
B. Interoperability
C. Availability
D. Security
Answer: A (LEAVE A REPLY)

NEW QUESTION: 325
Setting thermostat controls by measuring the temperature will result in the _____ highest energy costs.
Response:
A. Under-floor
B. Return air
C. External ambient
D. Server inlet
Answer: B (LEAVE A REPLY)

NEW QUESTION: 326
BCDR strategies do not typically involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the amount of services that need to be recovered to meet BCDR objectives?
A. RSL
B. RTO
C. RPO

D. SRE

Answer: (SHOW ANSWER)

Explanation

The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the determined level of operations necessary during a BCDR situation.

The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. SRE is provided as an erroneous response.

NEW QUESTION: 327

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

A. Limit

B. Cap

C. Throttle

D. Reservation

Answer: A (LEAVE A REPLY)

A limit puts a maximum value on the amount of resources that may be consumed by either a system, a service, or a cloud customer. It is commonly used to prevent one entity from consuming enormous amounts of resources and having an operational impact on other tenants within the same cloud system.

Limits can either be hard or somewhat flexible, meaning a customer can borrow from other customers while still having their actual limit preserved. A reservation is a guarantee to a cloud customer that a certain level of resources will always be available to them, regardless of what operational demands are currently placed on the cloud environment.

Both cap and throttle are terms that sound similar to limit, but they are not the correct terms in this case.

NEW QUESTION: 328

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

A. Community

B. Hybrid

C. Private

D. Public

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

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

NEW QUESTION: 329
When an API is being leveraged, it will encapsulate its data for transmission back to the requesting party or service.
What is the data encapsulation used with the SOAP protocol referred to as?
A. Packet
B. Payload
C. Object
D. Envelope
Answer: (SHOW ANSWER)
Explanation
Simple Object Access Protocol (SOAP) encapsulates its information in what is known as a SOAP envelope. It then leverages common communications protocols for transmission. Object is a type of cloud storage, but also a commonly used term with certain types of programming languages. Packet and payload are terms that sound similar to envelope but are not correct in this case.

NEW QUESTION: 330
Which type of cloud model typically presents the most challenges to a cloud customer during the "destroy" phase of the cloud data lifecycle?
A. IaaS
B. DaaS
C. SaaS
D. PaaS
Answer: (SHOW ANSWER)
Explanation
With many SaaS implementations, data is not isolated to a particular customer but rather is part of the overall application. When it comes to data destruction, a particular challenge is ensuring that all of a customer's data is completely destroyed while not impacting the data of other customers.

NEW QUESTION: 331
Which of the following is NOT something that an HIDS will monitor?
A. Configurations
B. User logins
C. Critical system files
D. Network traffic
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 332
Which component of ITIL involves the creation of an RFC ticket and obtaining official approvals for it?
A. Problem management
B. Release management
C. Deployment management
D. Change management
Answer: (SHOW ANSWER)
Explanation
The change management process involves the creation of the official Request for Change (RFC) ticket, which is used to document the change, obtain the required approvals from management and stakeholders, and track the change to completion. Release management is a subcomponent of change management, where the actual code or configuration change is put into place. Deployment management is similar to release management, but it's where changes are actually implemented on systems. Problem management is focused on the identification and mitigation of known problems and deficiencies before they are able to occur.

NEW QUESTION: 333
Which of the following roles involves the connection and integration of existing systems and services to a cloud environment?
A. Cloud service business manager
B. Cloud service user
C. Cloud service administrator
D. Cloud service integrator
Answer: D (LEAVE A REPLY)
The cloud service integrator is the official role that involves connecting and integrating existing systems and services with a cloud environment. This may involve moving services

into a cloud environment, or connecting to external cloud services and capabilities from traditional data center-hosted services.

NEW QUESTION: 334
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 (LEAVE A REPLY)
Explanation/Reference:
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: 335
Which of the following methods of addressing risk is most associated with insurance?
Response:
A. Acceptance
B. Avoidance
C. Transference
D. Mitigation
Answer: (SHOW ANSWER)

NEW QUESTION: 336
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 (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Print spooling is not a metric for system performance; all the rest are.

NEW QUESTION: 337
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 (LEAVE A REPLY)
Explanation/Reference:
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: 338
Which of the following is NOT a core component of an SIEM solution?
A. Escalation
B. Correlation
C. Compliance
D. Aggregation
Answer: (SHOW ANSWER)

NEW QUESTION: 339
Static software security testing typically uses _____ as a measure of how thorough the testing was.
A. Code coverage
B. Number of testers
C. Malware hits
D. Flaws detected
Answer: (SHOW ANSWER)

NEW QUESTION: 340
Which of the following are the storage types associated with PaaS?
A. Structured and freeform
B. Volume and object
C. Structured and unstructured
D. Database and file system
Answer: C (LEAVE A REPLY)
Explanation

NEW QUESTION: 341
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. Crypthographic erasure

D. Overwriting
Answer: C (LEAVE A REPLY)
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: 342
How many additional DNS queries are needed when DNSSEC integrity checks are added?
A. Three
B. Zero
C. One
D. Two
Answer: B (LEAVE A REPLY)
Explanation
DNSSEC does not require any additional DNS queries to be performed. The DNSSEC integrity checks and validations are all performed as part of the single DNS lookup resolution.

NEW QUESTION: 343
Which of the following is the correct name for Tier II of the Uptime Institute Data Center Site Infrastructure Tier Standard Topology?
A. Basic Site Infrastructure
B. Fault-Tolerant Site Infrastructure
C. Concurrently Maintainable Site Infrastructure
D. Redundant Site Infrastructure Capacity Components
Answer: D (LEAVE A REPLY)

NEW QUESTION: 344
What is the minimum regularity for testing a BCDR plan to meet best practices?
A. Once year
B. Once a month
C. Every six months
D. When the budget allows it
Answer: (SHOW ANSWER)

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

NEW QUESTION: 345
Deviations from the baseline should be investigated and _____.
A. Revealed
B. Documented
C. Encouraged
D. Enforced
Answer: B (LEAVE A REPLY)
Explanation/Reference:
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: 346
Firewalls are used to provide network security throughout an enterprise and to control what information can be accessed--and to a certain extent, through what means.
Which of the following is NOT something that firewalls are concerned with?
A. IP address
B. Encryption
C. Port
D. Protocol
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Firewalls work at the network level and control traffic based on the source, destination, protocol, and ports.
Whether or not the traffic is encrypted is not a factor with firewalls and their decisions about routing traffic.
Firewalls work primarily with IP addresses, ports, and protocols.

NEW QUESTION: 347
With a federated identity system, where would a user perform their authentication when requesting services or application access?
A. Cloud provider
B. The application
C. Their home organization
D. Third-party authentication system
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
With a federated identity system, a user will perform authentication with their home organization, and the application will accept the authentication tokens and user information from the identity provider in order to grant access. The purpose of a federated system is to allow users to authenticate from their home organization. Therefore, using the application or a third-party authentication system would be contrary to the purpose of a federated system because it necessitates the creation of additional accounts. The use of a cloud provider would not be relevant to the operations of a federated system.

NEW QUESTION: 348
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 (LEAVE A REPLY)
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: 349
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 (LEAVE A REPLY)
The other options are the names of the phases, but out of proper order.

NEW QUESTION: 350
What is the intellectual property protection for a useful manufacturing innovation?
A. Trademark
B. Copyright
C. patent
D. Trade secret
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Patents protect processes (as well as inventions, new plantlife, and decorative patterns).
The other answers listed are answers to other questions.

NEW QUESTION: 351
What does nonrepudiation mean?
A. Ensuring that a transaction is completed before saving the results
B. Ensuring that someone cannot turn off auditing capabilities while performing a function
C. Preventing any party that participates in a transaction from claiming that it did not
D. Prohibiting certain parties from a private conversation
Answer: (SHOW ANSWER)

NEW QUESTION: 352
A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence.
Which core concept of cloud computing is most related to vendor lock-in?
A. Scalability
B. Interoperability
C. Portability
D. Reversibility
Answer: C (LEAVE A REPLY)
Portability is the ability for a cloud customer to easily move their systems, services, and applications among different cloud providers. By avoiding reliance on proprietary APIs and other vendor-specific cloud features, an organization can maintain flexibility to move among the various cloud providers with greater ease.
Reversibility refers to the ability for a cloud customer to quickly and easy remove all their services and data from a cloud provider. Interoperability is the ability to reuse services and components for other applications and uses. Scalability refers to the ability of a cloud environment to add or remove resources to meet current demands.

NEW QUESTION: 353
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 (LEAVE A REPLY)
Explanation/Reference:
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: 354
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 (LEAVE A REPLY)
Explanation/Reference:
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: 355
From a legal perspective, what is the most important first step after an eDiscovery order has been received by the cloud provider?

A. Notification
B. Key identification
C. Data collection
D. Virtual image snapshots
Answer: (SHOW ANSWER)
Explanation
The contract should include requirements for notification by the cloud provider to the cloud customer upon the receipt of such an order. This serves a few important purposes. First, it keeps communication and trust open between the cloud provider and cloud customers. Second, and more importantly, it allows the cloud customer to potentially challenge the order if they feel they have the grounds or desire to do so.

NEW QUESTION: 356
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "cross-site scripting (XSS)." Which of the following is not a method for reducing the risk of XSS attacks?
Response:
A. Sanitize HTML markup with a library designed for the purpose.
B. XML escape all identity assertions.
C. Use an auto-escaping template system.
D. HTML escape JSON values in an HTML context and read the data with JSON.parse.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 357
At which layer does the IPSec protocol operate to encrypt and protect communications between two parties?
Response:
A. Data link
B. Transport
C. Network
D. Application
Answer: C (LEAVE A REPLY)

NEW QUESTION: 358
Security is a critical yet often overlooked consideration for BCDR planning.
At which stage of the planning process should security be involved?
A. Scope definition
B. Requirements gathering
C. Analysis

D. Risk assessment

Answer: (SHOW ANSWER)

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

NEW QUESTION: 359

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

A. Metadata

B. Content analysis

C. Labels

D. ACLs

Answer: A (LEAVE A REPLY)

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: 360

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 (LEAVE A REPLY)

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

NEW QUESTION: 361

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

A. Service level agreement

B. Service level contract

C. Service compliance contract

D. Service level amendment

Answer: A (LEAVE A REPLY)

Explanation/Reference:

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

NEW QUESTION: 362
What is the only data format permitted with the SOAP API?
A. HTML
B. SAML
C. XSML
D. XML
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The SOAP protocol only supports the XML data format.

NEW QUESTION: 363
DLP solutions typically involve all of the following aspects except _____.
Response:
A. Enforcement
B. Tokenization
C. Monitoring
D. Data discovery
Answer: B (LEAVE A REPLY)

NEW QUESTION: 364
Which of the following threat types can occur when baselines are not appropriately applied or when unauthorized changes are made?
A. Security misconfiguration
B. Insecure direct object references
C. Unvalidated redirects and forwards

D. Sensitive data exposure
Answer: (SHOW ANSWER)
Explanation
Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner. This can be due to a shortcoming in security baselines or configurations, unauthorized changes to system configurations, or a failure to patch and upgrade systems as the vendor releases security patches. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, allowing spoofing for malware or phishing attacks. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data.

NEW QUESTION: 365
Which of the following storage types is most closely associated with a traditional file system and tree structure?
A. Volume
B. Unstructured
C. Object
D. Structured
Answer: A (LEAVE A REPLY)
Explanation
Volume storage works as a virtual hard drive that is attached to a virtual machine. The operating system sees the volume the same as how a traditional drive on a physical server would be seen.

NEW QUESTION: 366
Your organization has made it a top priority that any cloud environment being considered to host production systems have guarantees that resources will always be available for allocation when needed.
Which of the following concepts will you need to ensure is part of the contract and SLA?
A. Resource pooling
B. Limits
C. Shares
D. Reservations
Answer: D (LEAVE A REPLY)

NEW QUESTION: 367

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 (LEAVE A REPLY)
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: 368
Resolving resource contentions in the cloud will most likely be the job of the _____.
Response:
A. Router
B. Emulator
C. Hypervisor
D. Regulator
Answer: C (LEAVE A REPLY)

NEW QUESTION: 369
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 (LEAVE A REPLY)
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: 370
Which is the appropriate phase of the cloud data lifecycle for determining the data's classification?
A. Create
B. Use
C. Share
D. Store
Answer: (SHOW ANSWER)
Any time data is created, modified, or imported, the classification needs to be evaluated and set from the earliest phase to ensure security is always properly maintained for the duration of its lifecycle.

NEW QUESTION: 371
Which of the following represents a minimum guaranteed resource within a cloud environment for the cloud customer?
A. Reservation
B. Share
C. Limit
D. Provision
Answer: A (LEAVE A REPLY)
A reservation is a minimum resource that is guaranteed to a customer within a cloud environment. Within a cloud, a reservation can pertain to the two main aspects of computing: memory and processor. With a reservation in place, the cloud provider guarantees that a cloud customer will always have at minimum the necessary resources available to power on and operate any of their services.

NEW QUESTION: 372
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 (LEAVE A REPLY)

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: 373
A user signs on to a cloud-based social media platform. In another browser tab, the user finds an article worth posting to the social media platform. The user clicks on the platform's icon listed on the article's website, and the article is automatically posted to the user's account on the social media platform.
This is an example of what?
Response:
A. Identity federation
B. Cross-site scripting
C. Insecure direct identifiers
D. Single sign-on
Answer: A (LEAVE A REPLY)

NEW QUESTION: 374
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 (LEAVE A REPLY)
Explanation/Reference:
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: 375
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 supports. 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.

B. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the provider supports. 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.
C. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the consumer supports. 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.
D. To deploy onto the cloud infrastructure provider-created or acquired applications created using programming languages, libraries, services, and tools that the provider supports. 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: (SHOW ANSWER)
Explanation/Reference:
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: 376
Data center and operations design traditionally takes a tiered, topological approach. Which of the following standards is focused on that approach and is prevalently used throughout the industry?
A. IDCA
B. NFPA
C. BICSI
D. Uptime Institute
Answer: D (LEAVE A REPLY)
Explanation
The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers.

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

NEW QUESTION: 377
DLP solutions typically involve all of the following aspects except _____.
A. Tokenization
B. Monitoring
C. Data discovery
D. Enforcement
Answer: A (LEAVE A REPLY)

NEW QUESTION: 378
A comprehensive BCDR plan will encapsulate many or most of the traditional concerns of operating a system in any data center.
However, what is one consideration that is often overlooked with the formulation of a BCDR plan?
A. Availability of staff
B. Capacity at the BCDR site
C. Restoration of services
D. Change management processes
Answer: C (LEAVE A REPLY)
Explanation
BCDR planning tends to focus so much on the failing over of services in the case of a disaster that recovery back to primary hosting after the disaster is often overlooked. In many instances, this can be just as complex a process as failing over, if not more so. Availability of staff, capacity at the BCDR site, and change management processes are typically integral to BCDR plans and are common components of them.

NEW QUESTION: 379

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

A. Volume

B. Unstructured

C. Object

D. Structured

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 380

Many activities within a cloud environment are performed via programmatic means, where complex and distributed operations are handled without the need to perform each step individually.

Which of the following concepts does this describe?

A. Orchestration

B. Provisioning

C. Automation

D. Allocation

Answer: (SHOW ANSWER)

Orchestration is the programmatic means of managing and coordinating activities within a cloud environment and allowing for a commensurate level of automation and self-service. Provisioning, allocation, and automation are all components of orchestration, but none refers to the overall concept.

NEW QUESTION: 381

Which of the following data-sanitation approaches are always available within a cloud environment?

Response:

A. Overwriting

B. Cryptographic erasure

C. Physical destruction

D. Shredding

Answer: (SHOW ANSWER)

NEW QUESTION: 382

What type of masking strategy involves making a separate and distinct copy of data with masking in place?

A. Dynamic

B. Replication

C. Static
D. Duplication
Answer: C (LEAVE A REPLY)
With static masking, a separate and distinct copy of the data set is created with masking in place. This is typically done through a script or other process that takes a standard data set, processes it to mask the appropriate and predefined fields, and then outputs the data set as a new one with the completed masking done.

NEW QUESTION: 383
Which of the following is a risk associated with manual patching especially in the cloud?
Response:
A. No notice before the impact is realized
B. Lack of applicability to the environment
C. The possibility for human error
D. Patches may or may not address the vulnerability they were designed to fix.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 384
Many different common threats exist against web-exposed services and applications. One attack involves attempting to leverage input fields to execute queries in a nested fashion that is unintended by the developers.
What type of attack is this?
A. Injection
B. Missing function-level access control
C. Cross-site scripting
D. Cross-site request forgery
Answer: A (LEAVE A REPLY)
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. This can trick an application into exposing data that is not intended or authorized to be exposed, or it can potentially allow an attacker to gain insight into configurations or security controls. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.
Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes.

NEW QUESTION: 385

Three central concepts define what type of data and information an organization is responsible for pertaining to eDiscovery.
Which of the following are the three components that comprise required disclosure?
A. Possession, ownership, control
B. Ownership, use, creation
C. Control, custody, use
D. Possession, custody, control
Answer: D (LEAVE A REPLY)
Data that falls under the purview of an eDiscovery request is that which is in the possession, custody, or control of the organization. Although this is an easy concept in a traditional data center, it can be difficult to distinguish who actually possesses and controls the data in a cloud environment due to multitenancy and resource pooling. Although these options provide similar- sounding terms, they are ultimately incorrect.

NEW QUESTION: 386
In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?
A. HIPAA
B. The contract
C. Statutes
D. Security control matrix
Answer: (SHOW ANSWER)
Explanation
The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable. The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

NEW QUESTION: 387
Which of the following concepts is NOT one of the core components to an encryption system architecture?
A. Software
B. Network
C. Keys
D. Data
Answer: B (LEAVE A REPLY)
Explanation
Explanation:

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

NEW QUESTION: 388
Which cloud service category offers the most customization options and control to the cloud customer?
A. SaaS
B. PaaS
C. IaaS
D. DaaS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 389
What type of data does data rights management (DRM) protect?
A. Consumer
B. PII
C. Financial
D. Healthcare
Answer: (SHOW ANSWER)
DRM applies to the protection of consumer media, such as music, publications, video, movies, and soon.

NEW QUESTION: 390
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: (SHOW ANSWER)
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: 391
What is the only data format permitted with the SOAP API?
A. HTML
B. SAML
C. XSML
D. XML
Answer: D (LEAVE A REPLY)
The SOAP protocol only supports the XML data format.

NEW QUESTION: 392
Which jurisdiction lacks specific and comprehensive privacy laws at a national or top level of legal authority?
A. European Union
B. Germany
C. Russia
D. United States
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The United States lacks a single comprehensive law at the federal level addressing data security and privacy, but there are multiple federal laws that deal with different industries.

NEW QUESTION: 393
What is the intellectual property protection for the tangible expression of a creative idea?
A. Trade secret
B. Copyright
C. Trademark
D. Patent
Answer: (SHOW ANSWER)

Explanation
Copyrights are protected tangible expressions of creative works. The other answers listed are answers to subsequent questions.

NEW QUESTION: 394
Which is the lowest level of the CSA STAR program?
A. Attestation
B. Self-assessment
C. Hybridization
D. Continuous monitoring
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The lowest level is Level 1, which is self-assessment, Level 2 is an external third-party attestation, and Level 3 is a continuous-monitoring program. Hybridization does not exist as part of the CSA STAR program.

NEW QUESTION: 395
_____ is the legal concept whereby a cloud customer is held to a reasonable expectation for providing security of its users' and clients' privacy data in their control.
Response:
A. Reciprocity
B. Due diligence
C. Due care
D. Liability
Answer: (SHOW ANSWER)

NEW QUESTION: 396
Which of the following is a file server that provides data access to multiple, heterogeneous machines/users on the network?
Response:
A. Storage area network (SAN)
B. Hardware security module (HSM)
C. Content delivery network (CDN)
D. Network-attached storage (NAS)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 397
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 (LEAVE A REPLY)
Explanation
Structured storage involves organized and categorized data, which most closely resembles and operates like a database system would.

NEW QUESTION: 398
What is the main reason virtualization is used in the cloud?
Response:
A. VMs are easier to administer
B. With VMs, the cloud provider does not have to deploy an entire hardware device for every new user
C. If a VM is infected with malware, it can be easily replaced
D. VMs are easier to operate than actual devices
Answer: (SHOW ANSWER)

NEW QUESTION: 399
Which of the following threat types can occur when encryption is not properly applied or insecure transport mechanisms are used?
A. Security misconfiguration
B. Insecure direct object references
C. Sensitive data exposure
D. Unvalidated redirects and forwards
Answer: C (LEAVE A REPLY)
Sensitive data exposure occurs when information is not properly secured through encryption and secure transport mechanisms; it can quickly become an easy and broad method for attackers to compromise information. Web applications must enforce strong encryption and security controls on the application side, but secure methods of communications with browsers or other clients used to access the information are also required. Security misconfiguration occurs when applications and systems are not properly configured for security, often a result of misapplied or inadequate baselines. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, thus allowing spoofing for malware or phishing attacks.

NEW QUESTION: 400

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

A. Quantity

B. Language

C. Quality

D. Number of courses

Answer: C (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 401

Which of the following roles involves testing, monitoring, and securing cloud services for an organization?

A. Cloud service integrator

B. Cloud service business manager

C. Cloud service user

D. Cloud service administrator

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The cloud service administrator is responsible for testing cloud services, monitoring services, administering security for services, providing usage reports on cloud services, and addressing problem reports

NEW QUESTION: 402

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

A. Labels

B. Quality

C. Volume

D. Format

Answer: B (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 403
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 (LEAVE A REPLY)
Explanation/Reference:
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: 404
Which of the following threat types involves an application developer leaving references to internal information and configurations in code that is exposed to the client?
A. Sensitive data exposure
B. Security misconfiguration
C. Insecure direct object references
D. Unvalidated redirect and forwards
Answer: C (LEAVE A REPLY)
An insecure direct object reference occurs when a developer has in their code a reference to something on the application side, such as a database key, the directory structure of the application, configuration information about the hosting system, or any other information that pertains to the workings of the application that should not be exposed to users or the network. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, allowing spoofing for malware of phishing attacks.
Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data. Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner.

NEW QUESTION: 405

The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "using components with known vulnerabilities." Why would an organization ever use components with known vulnerabilities to create software?
Response:
A. The particular vulnerabilities only exist in a context not being used by developers.
B. A component might have a hidden vulnerability.
C. The organization is insured.
D. Some vulnerabilities only exist in foreign countries.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 406
Which of the following standards primarily pertains to cabling designs and setups in a data center?
A. IDCA
B. BICSI
C. NFPA
D. Uptime Institute
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The standards put out by Building Industry Consulting Service International (BICSI) primarily cover complex cabling designs and setups for data centers, but also include specifications on power, energy efficiency, and hot/cold aisle setups.

NEW QUESTION: 407
Your organization is considering a move to a cloud environment and is looking for certifications or audit reports from cloud providers to ensure adequate security controls and processes.
Which of the following is NOT a security certification or audit report that would be pertinent?

Response:
A. SOC Type 2
B. FedRAMP
C. PCI DSS
D. FIPS 140-2
Answer: D (LEAVE A REPLY)

NEW QUESTION: 408
Who should be involved in review and maintenance of user accounts/access?
A. The user's manager
B. The security manager
C. The incident response team
D. The accounting department
Answer: A (LEAVE A REPLY)

NEW QUESTION: 409
A localized incident or disaster can be addressed in a cost-effective manner by using which of the following?
A. UPS
B. Generators
C. Joint operating agreements
D. Strict adherence to applicable regulations
Answer: C (LEAVE A REPLY)
Joint operating agreements can provide nearby relocation sites so that a disruption limited to the organization's own facility and campus can be addressed at a different facility and campus. UPS and generators are not limited to serving needs for localized causes. Regulations do not promote cost savings and are not often the immediate concern during BC/DR activities.

NEW QUESTION: 410
Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?
Response:
A. Data
B. Cash
C. Personnel
D. Systems
Answer: B (LEAVE A REPLY)

NEW QUESTION: 411

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 (LEAVE A REPLY)

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: 412

What process is used within a cloud environment to maintain resource balancing and ensure that resources are available where and when needed?

A. Dynamic clustering

B. Dynamic balancing

C. Dynamic resource scheduling

D. Dynamic optimization

Answer: D (LEAVE A REPLY)

Dynamic optimization is the process through which the cloud environment is constantly maintained to ensure resources are available when and where needed, and that physical nodes do not become overloaded or near capacity, while others are underutilized.

NEW QUESTION: 413

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

A. When it is behind a WAF

B. When it is behind an IPS

C. When it is not patched

D. When it is powered off

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

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

NEW QUESTION: 414
Which technology is NOT commonly used for security with data in transit?
A. DNSSEC
B. IPsec
C. VPN
D. HTTPS
Answer: A (LEAVE A REPLY)
Explanation
DNSSEC relates to the integrity of DNS resolutions and the prevention of spoofing or redirection, and does not pertain to the actual security of transmissions or the protection of data.

NEW QUESTION: 415
What is the best approach for dealing with services or utilities that are installed on a system but not needed to perform their desired function?
A. Remove
B. Monitor
C. Disable
D. Stop
Answer: A (LEAVE A REPLY)
Explanation
The best practice is to totally remove any unneeded services and utilities on a system to prevent any chance of compromise or use. If they are just disabled, it is possible for them to be inadvertently started again at any point, or another exploit could be used to start them again. Removing also negates the need to patch and maintain them going forward.

NEW QUESTION: 416
Cryptographic keys for encrypted data stored in the cloud should be _____.
Response:
A. Split into groups
B. Generated with redundancy
C. At least 128 bits long
D. Not stored with the cloud provider
Answer: D (LEAVE A REPLY)

NEW QUESTION: 417
Which of the following is NOT a regulatory system from the United States federal government?
A. PCI DSS
B. FISMA
C. SOX

D. HIPAA
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The payment card industry data security standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry regulatory standard, not a governmental one.

NEW QUESTION: 418
Which aspect of cloud computing makes it very difficult to perform repeat audits over time to track changes and compliance?
A. Virtualization
B. Multitenancy
C. Resource pooling
D. Dynamic optimization
Answer: A (LEAVE A REPLY)
Explanation
Cloud environments will regularly change virtual machines as patching and versions are changed. Unlike a physical environment, there is little continuity from one period of time to another. It is very unlikely that the same virtual machines would be in use during a repeat audit.

NEW QUESTION: 419
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 (LEAVE A REPLY)
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: 420
Which of the following would NOT be included as input into the requirements gathering for an application or system?
A. Users
B. Auditors

C. Management
D. Regulators
Answer: B (LEAVE A REPLY)

NEW QUESTION: 421
Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?
A. Hybrid
B. Public
C. Private
D. Community
Answer: B (LEAVE A REPLY)
Explanation
Popular services such as iCloud, Dropbox, and OneDrive are all publicly available and are open to any user for free, with possible add-on services offered for a cost.

NEW QUESTION: 422
Bob is staging an attack against Alice's website. He is able to embed a link on her site that will execute malicious code on a visitor's machine, if the visitor clicks on the link. This is an example of which type of attack?
Response:
A. Broken authentication/session management
B. Security misconfiguration
C. Insecure cryptographic storage
D. Cross-site scripting
Answer: D (LEAVE A REPLY)

NEW QUESTION: 423
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 (LEAVE A REPLY)
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: 424
All of the following entitles are required to use FedRAMP-accredited Cloud Service Providers except _____.
Response:
A. The CIA
B. The US post office
C. The Department of Homeland Security
D. Federal Express
Answer: D (LEAVE A REPLY)

NEW QUESTION: 425
Which of the following could be used as a second component of multifactor authentication if a user has an RSA token?
A. Access card
B. USB thumb drive
C. Retina scan
D. RFID
Answer: C (LEAVE A REPLY)
A retina scan could be used in conjunction with an RSA token because it is a biometric factor, and thus a different type of factor. An access card, RFID, and USB thumb drive are all items in possession of a user, the same as an RSA token, and as such would not be appropriate.

NEW QUESTION: 426
Which technology can be useful during the "share" phase of the cloud data lifecycle to continue to protect data as it leaves the original system and security controls?
A. IPS

B. WAF
C. DLP
D. IDS
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Data loss prevention (DLP) can be applied to data that is leaving the security enclave to continue to enforce access restrictions and policies on other clients and systems.

NEW QUESTION: 427
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: (SHOW ANSWER)
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: 428
The Restatement (Second) Conflict of Law refers to which of the following?
A. How jurisdictional disputes are settled
B. The basis for deciding which laws are most appropriate in a situation where conflicting laws exist
C. Whether local or federal laws apply in a situation
D. When judges restate the law in an opinion
Answer: B (LEAVE A REPLY)

NEW QUESTION: 429
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 (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 430

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

A. Cross-site request forgery

B. Missing function-level access control

C. Injection

D. Cross-site scripting

Answer: B (LEAVE A REPLY)

It is imperative that applications do checks when each function or portion of the application is accessed to ensure that the user is properly authorized. Without continual checks each time a function is accessed, an attacker could forge requests to access portions of the application where authorization has not been granted.

An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.

NEW QUESTION: 431

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 (LEAVE A REPLY)

Explanation

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: 432
Which of the following threat types involves an application that does not validate authorization for portions of itself after the initial checks?
A. Injection
B. Missing function-level access control
C. Cross-site request forgery
D. Cross-site scripting
Answer: (SHOW ANSWER)
Explanation
It is imperative that an application perform checks when each function or portion of the application is accessed, to ensure that the user is properly authorized to access it. Without continual checks each time a function is accessed, an attacker could forge requests to access portions of the application where authorization has not been granted.

NEW QUESTION: 433
What are the phases of a software development lifecycle process model?
A. Planning and requirements analysis, define, design, develop, testing, and maintenance
B. Planning and requirements analysis, design, define, develop, testing, and maintenance
C. Define, planning and requirements analysis, design, develop, testing, and maintenance
D. Planning and requirements analysis, define, design, testing, develop, and maintenance
Answer: (SHOW ANSWER)

NEW QUESTION: 434
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 (LEAVE A REPLY)
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: 435

BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the amount of data and services needed to reach the predetermined level of operations?
A. SRE
B. RPO
C. RSL
D. RTO
Answer: (SHOW ANSWER)
The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the predetermined level of operations necessary during a BCDR situation.
The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. SRE is provided as an erroneous response.

NEW QUESTION: 436
Which of the following is not one of the defined security controls domains within the Cloud Controls Matrix, published by the Cloud Security Alliance?
A. Financial
B. Identity and access management
C. Human resources
D. Mobile security
Answer: A (LEAVE A REPLY)

NEW QUESTION: 437
What does static application security testing (SAST) offer as a tool to the testers?
A. Production system scanning
B. Injection attempts
C. Source code access
D. Live testing

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

NEW QUESTION: 438
What is the biggest negative to leasing space in a data center versus building or maintain your own?
A. Costs
B. Control
C. Certification
D. Regulation
Answer: (SHOW ANSWER)
Explanation
When leasing space in a data center, an organization will give up a large degree of control as to how it is built and maintained, and instead must conform to the policies and procedures of the owners and operators of the data center.

NEW QUESTION: 439
You are the data manager for a retail company; you anticipate a much higher volume of sales activity in the final quarter of each calendar year than the other quarters. In order to handle these increased transactions, and to accommodate the temporary sales personnel you will hire for only that time period, you consider augmenting your internal, on-premises production environment with a cloud capability for a specific duration, and will return to operating fully on-premises after the period of increased activity.
This is an example of _____.
A. Cloud fragility
B. Cloud enhancement
C. Cloud bursting
D. Cloud framing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 440
Which value refers to the amount of time it takes to recover operations in a BCDR situation to meet management's objectives?
A. RSL
B. RPO
C. SRE
D. RTO
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:

The recovery time objective (RTO) is a measure of the amount of time it would take to recover operations in the event of a disaster to the point where management's objectives are met for BCDR.

NEW QUESTION: 441
You are the security manager for a company that is considering cloud migration to an IaaS environment. You are assisting your company's IT architects in constructing the environment. Which of the following options do you recommend?
Response:
A. Enhanced productivity without encryption
B. Use of a Type II hypervisor
C. Use of a Type I hypervisor
D. Unrestricted public access
Answer: (SHOW ANSWER)

NEW QUESTION: 442
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 (LEAVE A REPLY)
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: 443
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 (LEAVE A REPLY)
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: 444
Being in a cloud environment, cloud customers lose a lot of insight and knowledge as to how their data is stored and their systems are deployed.
Which concept from the ISO/IEC cloud standards relates to the necessity of the cloud provider to inform the cloud customer on these issues?
A. Disclosure
B. Transparency
C. Openness
D. Documentation
Answer: B (LEAVE A REPLY)
Explanation
Transparency is the official process by which a cloud provider discloses insight and information into its configurations or operations to the appropriate audiences. Disclosure, openness, and documentation are all terms that sound similar to the correct answer, but none of them is the correct term in this case.

NEW QUESTION: 445
Which cloud storage type requires special consideration on the part of the cloud customer to ensure they do not program themselves into a vendor lock-in situation?
A. Unstructured
B. Object
C. Volume
D. Structured
Answer: D (LEAVE A REPLY)
Structured storage is designed, maintained, and implemented by a cloud service provider as part of a PaaS offering. It is specific to that cloud provider and the way they have opted to implement systems, so special care is required to ensure that applications are not designed in a way that will lock the cloud customer into a specific cloud provider with that dependency. Unstructured storage for auxiliary files would not lock a customer into a

specific provider. With volume and object storage, because the cloud customer maintains their own systems with IaaS, moving and replicating to a different cloud provider would be very easy.

NEW QUESTION: 446
The goals of SIEM solution implementation include all of the following, except:
A. Dashboarding
B. Performance enhancement
C. Trend analysis
D. Centralization of log streams
Answer: (SHOW ANSWER)
SIEM does not intend to provide any enhancement of performance; in fact, a SIEM solution may decrease performance because of additional overhead. All the rest are goals of SIEM implementations.

NEW QUESTION: 447
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: (SHOW ANSWER)
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: 448
What type of data does data rights management (DRM) protect?
A. Consumer
B. PII
C. Financial
D. Healthcare
Answer: A (LEAVE A REPLY)
Explanation
DRM applies to the protection of consumer media, such as music, publications, video, movies, and soon.

NEW QUESTION: 449
Which of the following threat types involves an application that does not validate authorization for portions of itself beyond when the user first enters it?

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

NEW QUESTION: 450
Which of the following is a possible negative aspect of bit-splitting?
A. Users will have far greater difficulty understanding the implementation.
B. Limited vendors make acquisition and support challenging.
C. There may be cause for management concern that the technology will violate internal policy.
D. It may require trust in additional third parties beyond the primary cloud service provider.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 451
Federation allows _____ across organizations.
Response:
A. Encryption
B. Access
C. Policy
D. Role replication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 452
The nature of cloud computing and how it operates make complying with data discovery and disclosure orders more difficult. Which of the following concepts provides the biggest challenge in regard to data collection, pursuant to a legal order?
Response:
A. Auto-scaling
B. Reversibility
C. Portability
D. Multitenancy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 453
Which of the following terms is NOT a commonly used category of risk acceptance?
A. Moderate
B. Critical
C. Minimal
D. Accepted
Answer: D (LEAVE A REPLY)
Explanation
Explanation
Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

NEW QUESTION: 454
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 (LEAVE A REPLY)
Legal controls are those controls that are designed to comply with laws and regulations whether they be local or international.

NEW QUESTION: 455
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing.
According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing?

Response:
A. Attackers have already published vulnerabilities for all known APIs.
B. Most of the cloud customer's interaction with resources will be performed through APIs.
C. APIs are inherently insecure.
D. APIs are known carcinogens.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 456
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 (LEAVE A REPLY)
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: 457
Which is the appropriate phase of the cloud data lifecycle for determining the data's classification?
A. Create
B. Use
C. Share
D. Store
Answer: A (LEAVE A REPLY)
Explanation
Any time data is created, modified, or imported, the classification needs to be evaluated and set from the earliest phase to ensure security is always properly maintained for the duration of its lifecycle.

NEW QUESTION: 458
Which of the cloud cross-cutting aspects relates to the ability for a cloud customer to easily remove their applications and data from a cloud environment?
A. Reversibility
B. Availability

C. Portability
D. Interoperability
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reversibility is the ability for a cloud customer to easily remove their applications or data from a cloud environment, as well as to ensure that all traces of their applications or data have been securely removed per a predefined agreement with the cloud provider.

NEW QUESTION: 459
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
In order to increase the security value of the DLP, you should consider combining it with _____.
Response:
A. An investment in upgraded project management software
B. Digital insurance policies
C. Digital rights management (DRM) and security event and incident management (SIEM) tools
D. The Uptime Institute's Tier certification
Answer: (SHOW ANSWER)

NEW QUESTION: 460
Which United States program was designed to enable organizations to bridge the gap between privacy laws and requirements of the United States and the European Union?
A. GLBA
B. HIPAA
C. Safe Harbor
D. SOX
Answer: C (LEAVE A REPLY)
Explanation
Due to the lack of an adequate privacy law or protection at the federal level in the United States, European privacy regulations generally prohibit the exporting or sharing of PII from Europe with the United States.
Participation in the Safe Harbor program is voluntary on behalf of an organization, but it does require them to conform to specific requirements and policies that mirror those from the EU. Thus, organizations can fulfill requirements for data sharing and export and possibly serve customers in the EU.

NEW QUESTION: 461
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: (SHOW ANSWER)
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: 462
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
Which of these activities should you perform before deploying the tool?
Response:
A. Harden all your routers
B. Survey your company's departments about the data under their control
C. Reconstruct your firewalls
D. Adjust the hypervisors
Answer: B (LEAVE A REPLY)

NEW QUESTION: 463
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 (LEAVE A REPLY)
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: 464

Federation should be _____ to the users.
Response:
A. Proportional
B. Expensive
C. Transparent
D. Hostile
Answer: C (LEAVE A REPLY)

NEW QUESTION: 465
Which of the following tools might be useful in data discovery efforts that are based on content analysis?
A. iSCSI
B. Digital Rights Management (DRM)
C. DLP
D. Fibre Channel over Ethernet (FCoE)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 466
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: (SHOW ANSWER)
Explanation/Reference:
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: 467
Jurisdictions have a broad range of privacy requirements pertaining to the handling of personal data and information.
Which jurisdiction requires all storage and processing of data that pertains to its citizens to be done on hardware that is physically located within its borders?
A. Japan
B. United States
C. European Union
D. Russia
Answer: D (LEAVE A REPLY)
Explanation
The Russian government requires all data and processing of information about its citizens to be done solely on systems and applications that reside within the physical borders of the country. The United States, European Union, and Japan focus their data privacy laws on requirements and methods for the protection of data, rather than where the data physically resides.

NEW QUESTION: 468
Halon is now illegal to use for data center fire suppression. What is the reason it was outlawed?
Response:
A. It causes undue damage to electronic systems.
B. It does not adequately suppress fires.
C. It can harm the environment.
D. It poses a threat to health and human safety when deployed.
Answer: (SHOW ANSWER)

NEW QUESTION: 469
Which of the following methods is often used to obscure data from production systems for use in test or development environments?
A. Classification
B. Encryption
C. Masking
D. Tokenization
Answer: C (LEAVE A REPLY)

NEW QUESTION: 470
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 (LEAVE A REPLY)
Explanation
Conflict of interest is a threat, not a control.

NEW QUESTION: 471
Which of the following are not examples of personnel controls?
A. Background checks
B. Strict access control mechanisms
C. Continuous security training
D. Reference checks
Answer: B (LEAVE A REPLY)

NEW QUESTION: 472
To address shared monitoring and testing responsibilities in a cloud configuration, the provider might offer all these to the cloud customer except:
A. Access to audit logs and performance data
B. DLP solution results
C. Security control administration
D. SIM, SEIM. and SEM logs
Answer: C (LEAVE A REPLY)
While the provider might share any of the other options listed, the provider will not share administration of security controls with the customer. Security controls are the sole province of the provider.

NEW QUESTION: 473
You are the security manager for a small application development company. Your company is considering the use of the cloud for software testing purposes. Which cloud service model is most likely to suit your needs?
Response:
A. LaaS
B. SaaS
C. IaaS
D. PaaS
Answer: (SHOW ANSWER)

NEW QUESTION: 474
Single sign-on systems work by authenticating users from a centralized location or using a centralized method, and then allowing applications that trust the system to grant those users access. What would be passed between the authentication system and the applications to grant a user access?
A. Certificate
B. Ticket
C. Token
D. Credential
Answer: (SHOW ANSWER)

NEW QUESTION: 475
Which cloud storage type resembles a virtual hard drive and can be utilized in the same manner and with the same type of features and capabilities?
A. Volume
B. Unstructured
C. Structured
D. Object
Answer: (SHOW ANSWER)
Volume storage is allocated and mounted as a virtual hard drive within IaaS implementations, and it can be maintained and used the same way a traditional file system can. Object storage uses a flat structure on remote services that is accessed via opaque descriptors, structured storage resembles database storage, and unstructured storage is used to hold auxiliary files in conjunction with applications hosted within a PaaS implementation.

NEW QUESTION: 476
Which of the following would NOT be included as input into the requirements gathering for an application or system?
Response:
A. Management
B. Auditors
C. Users
D. Regulators
Answer: B (LEAVE A REPLY)

NEW QUESTION: 477
Which of the following is a file server that provides data access to multiple, heterogeneous machines/users on the network?
A. Storage area network (SAN)

B. Hardware security module (HSM)
C. Content delivery network (CDN)
D. Network-attached storage (NAS)
Answer: (SHOW ANSWER)

NEW QUESTION: 478
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 (LEAVE A REPLY)
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: 479
Data center and operations design traditionally takes a tiered, topological approach. Which of the following standards is focused on that approach and is prevalently used throughout the industry?
A. IDCA
B. NFPA
C. BICSI
D. Uptime Institute
Answer: D (LEAVE A REPLY)
The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers.
The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The International Data Center Authority (IDCA) offers the Infinity Paradigm, which takes a macro-level approach to data center design.

NEW QUESTION: 480

You are a consultant performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost $24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant. The fire suppression system costs $15 million. An insurance policy that would cover the full replacement cost of the plant costs $1 million per month.
In order to establish the true annualized loss expectancy (ALE), you would need all of the following information except _____.
Response:
A. The length of time it would take to rebuild the plant
B. The amount of product the plant creates
C. The amount of revenue generated by the plant
D. The rate at which the plant generates revenue
Answer: (SHOW ANSWER)

NEW QUESTION: 481
Which of the following are not examples of personnel controls?
Response:
A. Strict access control mechanisms
B. Background checks
C. Reference checks
D. Continuous security training
Answer: A (LEAVE A REPLY)

NEW QUESTION: 482
What must SOAP rely on for security?
A. Encryption
B. Tokenization
C. TLS
D. SSL
Answer: A (LEAVE A REPLY)
Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for passing data, and it must rely on the encryption of those data packages for security.

NEW QUESTION: 483
Which of the following types of software is a Type 2 hypervisor dependent on that a Type 1 hypervisor isn't?
Response:
A. Operating system
B. IDS
C. VPN
D. Firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 484
Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality?
Response:
A. Masking
B. Obfuscation
C. Anonymization
D. Tokenization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 485
Many activities within a cloud environment are performed via programmatic means, where complex and distributed operations are handled without the need to perform each step individually.
Which of the following concepts does this describe?
A. Orchestration
B. Provisioning
C. Automation
D. Allocation
Answer: A (LEAVE A REPLY)
Explanation
Orchestration is the programmatic means of managing and coordinating activities within a cloud environment and allowing for a commensurate level of automation and self-service. Provisioning, allocation, and automation are all components of orchestration, but none refers to the overall concept.

NEW QUESTION: 486
Key maintenance and security are paramount within a cloud environment due to the widespread use of encryption for both data and transmissions.

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

A. Remote key management service

B. Local key management service

C. Client key management service

D. Internal key management service

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 487

A poorly negotiated cloud service contract could result in all the following detrimental effects except:

A. Malware

B. Vendor lock-in

C. Lack of necessary services

D. Unfavorable terms

Answer: A (LEAVE A REPLY)

NEW QUESTION: 488

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

A. Dynamic

B. Static

C. Replication

D. Duplication

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 489

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: (SHOW ANSWER)

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: 490

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

A. Data discovery

B. Masking

C. Tokenization

D. Obfuscation

Answer: A (LEAVE A REPLY)

NEW QUESTION: 491

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 (LEAVE A REPLY)

Explanation/Reference:

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: 492
Which of the following is NOT a focus or consideration of an internal audit?
A. Certification
B. Design
C. Costs
D. Operational efficiency
Answer: A (LEAVE A REPLY)
In order to obtain and comply with certifications, independent external audits must be performed and satisfied.
Although some testing of certification controls can be part of an internal audit, they will not satisfy requirements.

NEW QUESTION: 493
Which protocol operates at the network layer and provides for full point-to-point encryption of all communications and transmissions?
A. IPSec
B. VPN
C. SSL
D. TLS
Answer: A (LEAVE A REPLY)
IPSec is a protocol for encrypting and authenticating packets during transmission between two parties and can involve any type of device, application, or service. The protocol performs both the authentication and negotiation of security policies between the two parties at the start of the connection and then maintains these policies throughout the lifetime of the connection. TLS operates at the application layer, not the network layer, and is widely used to secure communications between two parties. SSL is similar to TLS but has been deprecated. Although a VPN allows a secure channel for communications into a private network from an outside location, it's not a protocol.

NEW QUESTION: 494
What type of software is often considered secured and validated via community knowledge?
A. Open source
B. Scripting
C. Proprietary
D. Object-oriented
Answer: A (LEAVE A REPLY)

NEW QUESTION: 495
What does a cloud customer purchase or obtain from a cloud provider?
A. Services

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

NEW QUESTION: 496
Which of the cloud cross-cutting aspects relates to the ability to reuse or move components of an application or service?
A. Availability
B. Interoperability
C. Reversibility
D. Portability
Answer: B (LEAVE A REPLY)
Interoperability is the ease with which one can move or reuse components of an application or service.
This is maximized when services are designed without specific dependencies on underlying platforms, operating systems, locations, or cloud providers.

NEW QUESTION: 497
Which of the following is NOT an application or utility to apply and enforce baselines on a system?
A. Chef
B. GitHub
C. Puppet
D. Active Directory
Answer: B (LEAVE A REPLY)

Explanation
GitHub is an application for code collaboration, including versioning and branching of code trees. It is not used for applying or maintaining system configurations.

NEW QUESTION: 498
DLP can be combined with what other security technology to enhance data controls?
A. DRM
B. Hypervisor
C. SIEM
D. Kerberos
Answer: A (LEAVE A REPLY)
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: 499
What is a form of cloud storage where data is stored as objects, arranged in a hierarchal structure, like a file tree?
Response:
A. Volume storage
B. Content delivery network (CDN)
C. Object storage
D. Databases
Answer: C (LEAVE A REPLY)

NEW QUESTION: 500
When a user accesses a system, what process determines the roles and privileges that user is granted within the application?
Response:
A. Authorization
B. Authentication
C. Provisioning
D. Privilege
Answer: A (LEAVE A REPLY)

NEW QUESTION: 501
What concept does the "D" represent with the STRIDE threat model?
A. Data loss
B. Denial of service

C. Data breach
D. Distributed
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Any application can be a possible target of denial-of-service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for non-authenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks.

NEW QUESTION: 502
If a key feature of cloud computing that your organization desires is the ability to scale and expand without limit or concern about available resources, which cloud deployment model would you MOST likely be considering?
A. Public
B. Hybrid
C. Private
D. Community
Answer: A (LEAVE A REPLY)
Explanation
Public clouds, such as AWS and Azure, are massive systems run by major corporations, and they account for a significant share of Internet traffic and services. They are always expanding, offer enormous resources to customers, and are the least likely to run into resource constraints compared to the other deployment models.
Private clouds would likely have the resources available for specific uses and could not be assumed to have a large pool of resources available for expansion. A community cloud would have the same issues as a private cloud, being targeted to similar organizations. A hybrid cloud, because it spans multiple clouds, would not fit the bill either, without the use of individual cloud models.

NEW QUESTION: 503
Which of the following service capabilities gives the cloud customer the most control over resources and configurations?
A. Desktop
B. Platform
C. Infrastructure
D. Software
Answer: C (LEAVE A REPLY)
Explanation

The infrastructure service capability gives the cloud customer substantial control in provisioning and configuring resources, including processing, storage, and network resources.

NEW QUESTION: 504
Which is the most commonly used standard for information exchange within a federated identity system?
Response:
A. OpenID
B. SAML
C. OAuth
D. WS-Federation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 505
A loosely coupled storage cluster will have performance and capacity limitations based on the

_____.
Response:
A. Total number of nodes in the cluster
B. Physical backplane connecting it
C. Amount of usage demanded
D. The performance and capacity in each node
Answer: (SHOW ANSWER)

NEW QUESTION: 506
Where is a DLP solution generally installed when utilized for monitoring data at rest?
A. Network firewall
B. Host system
C. Application server
D. Database server
Answer: B (LEAVE A REPLY)
To monitor data at rest appropriately, the DLP solution would be installed on the host system where the data resides. A database server, in some situations, may be an appropriate answer, but the host system is the best answer because a database server is only one example of where data could reside. An application server processes data and typically sits between the data and presentation zones, and as such, does not store data at rest. A network firewall would be more appropriate for data in transit because it is not a place where data would reside.

NEW QUESTION: 507

The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "unvalidated redirects and forwards." Which of the following is a good way to protect against this problem?

A. Don't use redirects/forwards in your applications.

B. Refrain from storing credentials long term.

C. Implement security incident/event monitoring (security information and event management (SIEM)/security information management (SIM)/security event management (SEM)) solutions.

D. Implement digital rights management (DRM) solutions.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 508

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

A. Cloud provider

B. The application

C. Their home organization

D. Third-party authentication system

Answer: C (LEAVE A REPLY)

With a federated identity system, a user will perform authentication with their home organization, and the application will accept the authentication tokens and user information from the identity provider in order to grant access. The purpose of a federated system is to allow users to authenticate from their home organization.

Therefore, using the application or a third-party authentication system would be contrary to the purpose of a federated system because it necessitates the creation of additional accounts. The use of a cloud provider would not be relevant to the operations of a federated system.

NEW QUESTION: 509

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: (SHOW ANSWER)

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: 510
Different security testing methodologies offer different strategies and approaches to testing systems, requiring security personnel to determine the best type to use for their specific circumstances.
What does dynamic application security testing (DAST) NOT entail that SAST does?
A. Discovery
B. Knowledge of the system
C. Scanning
D. Probing
Answer: B (LEAVE A REPLY)
Dynamic application security testing (DAST) is considered "black-box" testing and begins with no inside knowledge of the application or its configurations. Everything about it must be discovered during its testing. As with most types of testing, dynamic application security testing (DAST) involves probing, scanning, and a discovery process for system information.

NEW QUESTION: 511
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: (SHOW ANSWER)
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: 512
You are the security manager for a small surgical center. Your organization is reviewing upgrade options for its current, on-premises data center. In order to best meet your needs, which one of the following options would you recommend to senior management?
Response:
A. Building a completely new data center
B. Leasing a data center that is currently owned by another firm
C. Renting private cloud space in a Tier 2 data center
D. Staying with the current data center
Answer: A (LEAVE A REPLY)

NEW QUESTION: 513
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 (LEAVE A REPLY)
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: 514
Which of the following pertains to fire safety standards within a data center, specifically with their enormous electrical consumption?
A. NFPA
B. BICSI
C. IDCA
D. Uptime Institute

Answer: A (LEAVE A REPLY)
Explanation
The standards put out by the National Fire Protection Association (NFPA) cover general fire protection best practices for any type of facility, but also specific publications pertaining to IT equipment and data centers.

NEW QUESTION: 515
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 (LEAVE A REPLY)
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: 516
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 (LEAVE A REPLY)
Explanation/Reference:
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: 517
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 (LEAVE A REPLY)
Explanation/Reference:
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: 518
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: (SHOW ANSWER)
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: 519
Without the extensive funds of a large corporation, a small-sized company could gain considerable and cost-effective services for which of the following concepts by moving to a cloud environment?
A. Regulatory

B. Security
C. Testing
D. Development
Answer: B (LEAVE A REPLY)
Explanation
Cloud environments, regardless of the specific deployment model used, have extensive and robust security controls in place, especially in regard to physical and infrastructure security. A small company can leverage the extensive security controls and monitoring provided by a cloud provider, which they would unlikely ever be able to afford on their own.
Moving to a cloud would not result in any gains for development and testing because these areas require the same rigor regardless of where deployment and hosting occur.
Regulatory compliance in a cloud would not be a gain for an organization because it would likely result in additional oversight and auditing as well as require the organization to adapt to a new environment.

NEW QUESTION: 520
What is the best approach for dealing with services or utilities that are installed on a system but not needed to perform their desired function?
A. Remove
B. Monitor
C. Disable
D. Stop
Answer: (SHOW ANSWER)
The best practice is to totally remove any unneeded services and utilities on a system to prevent any chance of compromise or use. If they are just disabled, it is possible for them to be inadvertently started again at any point, or another exploit could be used to start them again.
Removing also negates the need to patch and maintain them going forward.

NEW QUESTION: 521
Which of the following threat types involves the sending of untrusted data to a user's browser to be executed with their own credentials and access?
A. Missing function level access control
B. Cross-site scripting
C. Cross-site request forgery
D. Injection
Answer: B (LEAVE A REPLY)
Explanation
Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or where the code is not properly escaped from processing by the browser. The code is then

executed on the user's browser with the user's own access and permissions, allowing an attacker to redirect their web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access.

NEW QUESTION: 522
You are the IT director for a small contracting firm. Your company is considering migrating to a cloud production environment.
Which service model would best fit your needs if you wanted an option that reduced the chance of vendor lock-in but also did not require the highest degree of administration by your own personnel?
Response:
A. SaaS
B. TanstaafL
C. IaaS
D. PaaS
Answer: (SHOW ANSWER)

NEW QUESTION: 523
Which value refers to the amount of data an organization would need to recover in the event of a BCDR situation in order to reach an acceptable level of operations?
A. SRE
B. RTO
C. RPO
D. RSL
Answer: C (LEAVE A REPLY)
Explanation
The recovery point objective (RPO) is defined as the amount of data a company would need to maintain and recover in order to function at a level acceptable to management. This may or may not be a restoration to full operating capacity, depending on what management deems as crucial and essential.

NEW QUESTION: 524
In a cloud environment, encryption should be used for all the following, except:
A. Secure sessions/VPN
B. Long-term storage of data
C. Near-term storage of virtualized images
D. Profile formatting
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:

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

NEW QUESTION: 525
Which jurisdiction lacks specific and comprehensive privacy laws at a national or top level of legal authority?
A. European Union
B. Germany
C. Russia
D. United States
Answer: D (LEAVE A REPLY)
Explanation
The United States lacks a single comprehensive law at the federal level addressing data security and privacy, but there are multiple federal laws that deal with different industries.

NEW QUESTION: 526
Which type of testing tends to produce the best and most comprehensive results for discovering system vulnerabilities?
Response:
A. Pen
B. Vulnerability
C. Static
D. Dynamic
Answer: C (LEAVE A REPLY)

NEW QUESTION: 527
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: (SHOW ANSWER)

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: 528

Which aspect of archiving must be tested regularly for the duration of retention requirements?

A. Availability

B. Recoverability

C. Auditability

D. Portability

Answer: B (LEAVE A REPLY)

In order for any archiving system to be deemed useful and compliant, regular tests must be performed to ensure the data can still be recovered and accessible, should it ever be needed, for the duration of the retention requirements.

NEW QUESTION: 529

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 (LEAVE A REPLY)

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: 530

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

A. Record

B. Binding

C. Negotiation

D. Handshake

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

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

NEW QUESTION: 531

Which protocol operates at the network layer and provides for full point-to-point encryption of all communications and transmissions?

A. IPSec

B. VPN

C. SSL

D. TLS

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

IPSec is a protocol for encrypting and authenticating packets during transmission between two parties and can involve any type of device, application, or service. The protocol performs both the authentication and negotiation of security policies between the two parties at the start of the connection and then maintains these policies throughout the lifetime of the connection. TLS operates at the application layer, not the network layer, and is widely used to secure communications between two parties. SSL is similar to TLS but has been deprecated. Although a VPN allows a secure channel for communications into a private network from an outside location, it's not a protocol.

NEW QUESTION: 532

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

A. Cross-site scripting

B. Missing function-level access control

C. Injection

D. Cross-site forgery

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 533
Which aspect of cloud computing makes data classification even more vital than in a traditional data center?
A. Interoperability
B. Virtualization
C. Multitenancy
D. Portability
Answer: (SHOW ANSWER)
Explanation
With multiple tenants within the same hosting environment, any failure to properly classify data may lead to potential exposure to other customers and applications within the same environment.

NEW QUESTION: 534
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 (LEAVE A REPLY)
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: 535
Which of the following is NOT a factor that is part of a firewall configuration?
A. Encryption
B. Port
C. Protocol
D. Source IP
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Firewalls take into account source IP, destination IP, the port the traffic is using, as well as the network protocol (UDP/TCP). Whether or not the traffic is encrypted is not something a firewall is concerned with.

NEW QUESTION: 536
What are third-party providers of IAM functions for the cloud environment?
A. AESs
B. SIEMs
C. DLPs
D. CASBs
Answer: (SHOW ANSWER)
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: 537
Many aspects and features of cloud computing can make eDiscovery compliance more difficult or costly.
Which aspect of cloud computing would be the MOST complicating factor?
A. Measured service
B. Broad network access
C. Multitenancy
D. Portability
Answer: C (LEAVE A REPLY)
Explanation
With multitenancy, multiple customers share the same physical hardware and systems. With the nature of a cloud environment and how it writes data across diverse systems that are shared by others, the process of eDiscovery becomes much more complicated. Administrators cannot pull physical drives or easily isolate which data to capture. They not only have to focus on which data they need to collect, while ensuring they find all of it, but

they also have to make sure that other data is not accidently collected and exposed along with it.
Measured service is the aspect of a cloud where customers only pay for the services they are actually using, and for the duration of their use. Portability refers to the ease with which an application or service can be moved among different cloud providers. Broad network access refers to the nature of cloud services being accessed via the public Internet, either with or without secure tunneling technologies. None of these concepts would pertain to eDiscovery.

NEW QUESTION: 538
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
Which of these activities should you perform before deploying the tool?
A. Harden all your routers
B. Adjust the hypervisors
C. Reconstruct your firewalls
D. Survey your company's departments about the data under their control
Answer: (SHOW ANSWER)

NEW QUESTION: 539
Which United States law is focused on accounting and financial practices of organizations?
A. Safe Harbor
B. GLBA
C. SOX
D. HIPAA
Answer: C (LEAVE A REPLY)
The Sarbanes-Oxley (SOX) Act is not an act that pertains to privacy or IT security directly, but rather regulates accounting and financial practices used by organizations. It was passed to protect stakeholders and shareholders from improper practices and errors, and it sets forth rules for compliance, regulated and enforced by the Securities and Exchange Commission (SEC). The main influence on IT systems and operations is the requirements it sets for data retention, specifically in regard to what types of records must be preserved and for how long.

NEW QUESTION: 540
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 (LEAVE A REPLY)
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: 541
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 (LEAVE A REPLY)
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: 542
Which term relates to the application of scientific methods and practices to evidence?
A. Forensics
B. Methodical
C. Theoretical
D. Measured
Answer: A (LEAVE A REPLY)
Explanation
Forensics is the application of scientific and methodical processes to identify, collect, preserve, analyze, and summarize/report digital information and evidence.

NEW QUESTION: 543

Which of the following should NOT be part of the requirement analysis phase of the software development lifecycle?

A. Functionality

B. Programming languages

C. Software platform

D. Security requirements

Answer: (SHOW ANSWER)

Security requirements should be incorporated into the software development lifecycle (SDLC) from the earliest requirement gathering stage and should be incorporated prior to the requirement analysis phase.

NEW QUESTION: 544

What is the term used to describe loss of access to data because the cloud provider has ceased operation?

Response:

A. Closing

B. Vendor lock-in

C. Masking

D. Vendor lock-out

Answer: (SHOW ANSWER)

NEW QUESTION: 545

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

A. Cloud service business manager

B. Cloud service deployment manager

C. Cloud service operations manager

D. Cloud service manager

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

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

NEW QUESTION: 546

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 (LEAVE A REPLY)
Explanation/Reference:
Explanation:
All the elements except adjudication need to be addressed in each policy. Adjudication is not an element of policy.

NEW QUESTION: 547
Which of the following is NOT a component of access control?
A. Accounting
B. Federation
C. Authorization
D. Authentication
Answer: B (LEAVE A REPLY)
Explanation
Federation is not a component of access control. Instead, it is used to allow users possessing credentials from other authorities and systems to access services outside of their domain. This allows for access and trust without the need to create additional, local credentials. Access control encompasses not only the key concepts of authorization and authentication, but also accounting. Accounting consists of collecting and maintaining logs for both authentication and authorization for operational and regulatory requirements.

NEW QUESTION: 548
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 (LEAVE A REPLY)
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: 549
Which of the following is an example of useful and sufficient data masking of the string "CCSP"?
Response:
A. TtLp
B. XCSP
C. PSCC

D. 3X91
Answer: A (LEAVE A REPLY)

NEW QUESTION: 550
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 (LEAVE A REPLY)
Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe. The rest are not.

NEW QUESTION: 551
Which SSAE 16 audit report is simply an attestation of audit results?
A. SOC 2, Type 1
B. SOC 1
C. SOC 2, Type 2
D. SOC 3
Answer: D (LEAVE A REPLY)

NEW QUESTION: 552
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 (LEAVE A REPLY)
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: 553
Which of the following best describes data masking?
A. A method for creating similar but inauthentic datasets used for software testing and user training.
B. A method used to protect prying eyes from data such as social security numbers and credit card data.

C. A method where the last few numbers in a dataset are not obscured. These are often used for authentication.
D. Data masking involves stripping out all digits in a string of numbers so as to obscure the original number.
Answer: A (LEAVE A REPLY)
Explanation
All of these answers are actually correct, but A is the best answer, because it is the most general, includes the others, and is therefore the optimum choice. This is a good example of the type of question that can appear on the actual exam.

NEW QUESTION: 554
Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:
Response:
A. The cloud provider's resellers
B. The cloud provider's vendors
C. The cloud provider's utilities
D. The cloud provider's suppliers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 555
In a Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a _____.
Response:
A. Domain name (DN)
B. Distinguished name (DN)
C. Default name (DN)
D. Directory name (DN)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 556
Why does a Type 2 hypervisor typically offer less security control than a Type 1 hypervisor?
A. A Type 2 hypervisor runs on top of another operating system and is dependent on the security of the OS for its own security.
B. A Type 2 hypervisor allows users to directly perform some functions with their own access.
C. A Type 2 hypervisor is open source, so attackers can more easily find exploitable vulnerabilities with that access.
D. A Type 2 hypervisor is always exposed to the public Internet for federated identity access.

Answer: A (LEAVE A REPLY)
A Type 2 hypervisor differs from a Type 1 hypervisor in that it runs on top of another operating system rather than directly tied into the underlying hardware of the virtual host servers. With this type of implementation, additional security and architecture concerns come into play because the interaction between the operating system and the hypervisor becomes a critical link. The hypervisor no longer has direct interaction and control over the underlying hardware, which means that some performance will be lost due to the operating system in the middle needing its own resources, patching requirements, and operational oversight.

NEW QUESTION: 557
Which value refers to the amount of time it takes to recover operations in a BCDR situation to meet management's objectives?
A. RSL
B. RPO
C. SRE
D. RTO
Answer: (SHOW ANSWER)
The recovery time objective (RTO) is a measure of the amount of time it would take to recover operations in the event of a disaster to the point where management's objectives are met for BCDR.

NEW QUESTION: 558
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 (LEAVE A REPLY)

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: 559

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

A. DRM

B. ITAR

C. EAR

D. EAL

Answer: (SHOW ANSWER)

ITAR is a Department of State program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Digital rights management tools are used for protecting electronic processing of intellectual property.

NEW QUESTION: 560

What is the intellectual property protection for a useful manufacturing innovation?

A. Trademark

B. Copyright

C. patent

D. Trade secret

Answer: C (LEAVE A REPLY)

Explanation

Patents protect processes (as well as inventions, new plantlife, and decorative patterns). The other answers listed are answers to other questions.

NEW QUESTION: 561

Deviations from the baseline should be investigated and _____.

A. Revealed

B. Documented

C. Encouraged

D. Enforced

Answer: (SHOW ANSWER)
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: 562
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: (SHOW ANSWER)
Explanation
All the answers are true, but B is the most complete.

NEW QUESTION: 563
Which document will enforce uptime and availability requirements between the cloud customer and cloud provider?
A. Service level agreement
B. Operational level agreement
C. Contract
D. Regulation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 564
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 (LEAVE A REPLY)
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: 565
Many tools and technologies are available for securing or monitoring data in transit within a data center, whether it is a traditional data center or a cloud.
Which of the following is NOT a technology for securing data in transit?
A. VPN
B. TLS
C. DNSSEC
D. HTTPS
Answer: C (LEAVE A REPLY)
Explanation
Explanation:
DNSSEC is an extension of the normal DNS protocol that enables a system to verify the integrity of a DNS query resolution by signing it from the authoritative source and verifying the signing chain. It is not used for securing data transmissions or exchanges. HTTPS is the most common method for securing web service and data calls within a cloud, and TLS is the current standard for encrypting HTTPS traffic. VPNs are widely used for securing data transmissions and service access.

NEW QUESTION: 566
Which of the following is not one of the types of controls?
Response:
A. Physical
B. Transitional
C. Administrative
D. Technical
Answer: B (LEAVE A REPLY)

NEW QUESTION: 567
Jurisdictions have a broad range of privacy requirements pertaining to the handling of personal data and information.
Which jurisdiction requires all storage and processing of data that pertains to its citizens to be done on hardware that is physically located within its borders?
A. Japan
B. United States
C. European Union
D. Russia
Answer: D (LEAVE A REPLY)

The Russian government requires all data and processing of information about its citizens to be done solely on systems and applications that reside within the physical borders of the country.
The United States, European Union, and Japan focus their data privacy laws on requirements and methods for the protection of data, rather than where the data physically resides.

NEW QUESTION: 568
Which data point that auditors always desire is very difficult to provide within a cloud environment?
A. Access policy
B. Systems architecture
C. Baselines
D. Privacy statement
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Cloud environments are constantly changing and often span multiple physical locations. A cloud customer is also very unlikely to have knowledge and insight into the underlying systems architecture in a cloud environment. Both of these realities make it very difficult, if not impossible, for an organization to provide a comprehensive systems design document.

NEW QUESTION: 569
Deviations from the baseline should be investigated and _____.
A. Revealed
B. Documented
C. Encouraged
D. Enforced
Answer: B (LEAVE A REPLY)
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: 570
Which of the following actions will NOT make data part of the create phase of the cloud data lifecycle?
A. Modify data
B. Modify metadata
C. New data
D. Import data

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

NEW QUESTION: 571
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 (LEAVE A REPLY)
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: 572
SOC Type 1 reports are considered "restricted use," in that they are intended only for limited audiences and purposes.
Which of the following is NOT a population that would be appropriate for a SOC Type 1 report?
A. Current clients

B. Auditors
C. Potential clients
D. The service organization
Answer: (SHOW ANSWER)
Potential clients are not served by SOC Type 1 audits. A Type 2 or Type 3 report would be appropriate for potential clients. SOC Type 1 reports are intended for restricted use, where only the service organization itself, current clients, or auditors would have access to them.

NEW QUESTION: 573
Many tools and technologies are available for securing or monitoring data in transit within a data center, whether it is a traditional data center or a cloud.
Which of the following is NOT a technology for securing data in transit?
A. VPN
B. TLS
C. DNSSEC
D. HTTPS
Answer: C (LEAVE A REPLY)
DNSSEC is an extension of the normal DNS protocol that enables a system to verify the integrity of a DNS query resolution by signing it from the authoritative source and verifying the signing chain. It is not used for securing data transmissions or exchanges. HTTPS is the most common method for securing web service and data calls within a cloud, and TLS is the current standard for encrypting HTTPS traffic. VPNs are widely used for securing data transmissions and service access.

NEW QUESTION: 574
Which cloud service category would be most ideal for a cloud customer that is developing software to test its applications among multiple hosting providers to determine the best option for its needs?
A. DaaS
B. PaaS
C. IaaS
D. SaaS
Answer: B (LEAVE A REPLY)
Platform as a Service would allow software developers to quickly and easily deploy their applications among different hosting providers for testing and validation in order to determine the best option. Although IaaS would also be appropriate for hosting applications, it would require too much configuration of application servers and libraries in order to test code. Conversely, PaaS would provide a ready-to-use environment from the onset. DaaS would not be appropriate in any way for software developers to use to deploy applications. IaaS would not be appropriate in this scenario because it would require the developers to also deploy and maintain the operating system images or to contract with

another firm to do so. SaaS, being a fully functional software platform, would not be appropriate for deploying applications into.

NEW QUESTION: 575
Which characteristic of automated patching makes it attractive?
Response:
A. Speed
B. Cost
C. Capability to recognize problems quickly
D. Noise reduction
Answer: A (LEAVE A REPLY)

NEW QUESTION: 576
Which of the following would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?
A. Resource pooling
B. Virtualization
C. Multitenancy
D. Regulation
Answer: (SHOW ANSWER)
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, and especially within a public cloud model, it is not possible or practical for a cloud provider to alter their services for specific customer demands.

NEW QUESTION: 577
Which of the following are cloud computing roles?
A. Cloud service broker and user
B. Cloud customer and financial auditor
C. CSP and backup service provider
D. Cloud service auditor and object
Answer: C (LEAVE A REPLY)
Explanation
The following groups form the key roles and functions associated with cloud computing. They do not constitute an exhaustive list but highlight the main roles and functions within cloud computing:
- Cloud customer: An individual or entity that utilizes or subscribes to cloud based services or resources.

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

NEW QUESTION: 578
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 (LEAVE A REPLY)
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: 579
Egress monitoring solutions usually include a function that _____.
Response:
A. Resides on client machines
B. Inspects incoming packets
C. Uses biometrics to scan users
D. Uses stateful inspection
Answer: (SHOW ANSWER)

NEW QUESTION: 580
Which security concept would business continuity and disaster recovery fall under?

A. Confidentiality
B. Availability
C. Fault tolerance
D. Integrity
Answer: B (LEAVE A REPLY)
Explanation
Disaster recovery and business continuity are vital concerns with availability. If data is destroyed or compromised, having regular backup systems in place as well as being able to perform disaster recovery in the event of a major or widespread problem allows operations to continue with an acceptable loss of time and data to management. This also ensures that sensitive data is protected and persisted in the event of the loss or corruption of data systems or physical storage systems.

NEW QUESTION: 581
Many different common threats exist against web-exposed services and applications. One attack involves attempting to leverage input fields to execute queries in a nested fashion that is unintended by the developers.
What type of attack is this?
A. Injection
B. Missing function-level access control
C. Cross-site scripting
D. Cross-site request forgery
Answer: A (LEAVE A REPLY)
Explanation
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. This can trick an application into exposing data that is not intended or authorized to be exposed, or it can potentially allow an attacker to gain insight into configurations or security controls. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.
Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes.

NEW QUESTION: 582
What is the primary reason that makes resolving jurisdictional conflicts complicated?
A. Different technology standards
B. Costs
C. Language barriers

D. Lack of international authority
Answer: D (LEAVE A REPLY)
Explanation
With international operations, systems ultimately cross many jurisdictional boundaries, and many times, they conflict with each other. The major hurdle to overcome for an organization is the lack of an ultimate international authority to mediate such conflicts, with a likely result of legal efforts in each jurisdiction.

NEW QUESTION: 583
If you're using iSCSI in a cloud environment, what must come from an external protocol or application?
A. Kerberos support
B. CHAP support
C. Authentication
D. Encryption
Answer: (SHOW ANSWER)
iSCSI does not natively support encryption, so another technology such as IPsec must be used to encrypt communications.

NEW QUESTION: 584
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 (LEAVE A REPLY)
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: 585
What expectation of data custodians is made much more challenging by a cloud implementation, especially with PaaS or SaaS?
A. Data classification
B. Knowledge of systems
C. Access to data
D. Encryption requirements
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 586
Which type of testing uses the same strategies and toolsets that hackers would use?
A. Static
B. Malicious
C. Penetration
D. Dynamic
Answer: C (LEAVE A REPLY)
Explanation
Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discovery potential vulnerabilities. Although the term malicious captures much of the intent of penetration testing from the perspective of an attacker, it is not the best answer. Static and dynamic are two types of system testing--where static is done offline and with knowledge of the system, and dynamic is done on a live system without any previous knowledge is associated--but neither describes the type of testing being asked for in the question.

NEW QUESTION: 587
Which component of ITIL pertains to planning, coordinating, executing, and validating changes and rollouts to production environments?
A. Release management
B. Availability management
C. Problem management
D. Change management
Answer: A (LEAVE A REPLY)
Release management involves planning, coordinating, executing, and validating changes and rollouts to the production environment. Change management is a higher-level

component than release management and also involves stakeholder and management approval, rather than specifically focusing the actual release itself. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION: 588
Audits are either done based on the status of a system or application at a specific time or done as a study over a period of time that takes into account changes and processes. Which of the following pairs matches an audit type that is done over time, along with the minimum span of time necessary for it?
A. SOC Type 2, one year
B. SOC Type 1, one year
C. SOC Type 2, one month
D. SOC Type 2, six months
Answer: D (LEAVE A REPLY)
SOC Type 2 audits are done over a period of time, with six months being the minimum duration.
SOC Type 1 audits are designed with a scope that's a static point in time, and the other times provided for SOC Type 2 are incorrect.

NEW QUESTION: 589
Which of the following represents a control on the maximum amount of resources that a single customer, virtual machine, or application can consume within a cloud environment?
A. Share
B. Reservation
C. Provision
D. Limit
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Limits are put in place to enforce a maximum on the amount of memory or processing a cloud customer can use. This can be done either on a virtual machine or as a comprehensive whole for a customer, and is meant to ensure that enormous cloud resources cannot be allocated or consumed by a single host or customer to the detriment of other hosts and customers.

NEW QUESTION: 590
Which of the following are cloud computing roles?
A. Cloud service broker and user
B. Cloud customer and financial auditor

C. CSP and backup service provider
D. Cloud service auditor and object
Answer: C (LEAVE A REPLY)
The following groups form the key roles and functions associated with cloud computing. They do not constitute an exhaustive list but highlight the main roles and functions within cloud computing:
- Cloud customer: An individual or entity that utilizes or subscribes to cloud based services or resources.
- CSP: A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations or individuals, usually for a fee; otherwise known to clients "as a service.
- Cloud backup service provider: A third-party entity that manages and holds operational responsibilities for cloud-based data backup services and solutions to customers from a central data center.
- CSB: Typically a third-party entity or company that looks to extend or enhance value to multiple customers of cloud-based services through relationships with multiple CSPs. It acts as a liaison between cloud services customers and CSPs, selecting the best provider for each customer and monitoring the services. The CSB can be utilized as a "middleman" to broker the best deal and customize services to the customer's requirements.
May also resell cloud services.
- Cloud service auditor: Third-party organization that verifies attainment of SLAs.

NEW QUESTION: 591
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: (SHOW ANSWER)
Explanation/Reference:
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: 592
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: (SHOW ANSWER)
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: 593
Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider?
Response:
A. SOC 2 Type 2
B. SOC 3
C. SOC 1 Type 2
D. SOC 1 Type 1
Answer: B (LEAVE A REPLY)

NEW QUESTION: 594
Egress monitoring solutions usually include a function that _____.
A. Uses biometrics to scan users
B. Resides on client machines
C. Inspects incoming packets
D. Uses stateful inspection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 595
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: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Team-building has nothing to do with SAST; all the rest of the answers are characteristics of SAST.

NEW QUESTION: 596
Which of the following is NOT a focus or consideration of an internal audit?
A. Certification
B. Design
C. Costs
D. Operational efficiency
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
In order to obtain and comply with certifications, independent external audits must be performed and satisfied. Although some testing of certification controls can be part of an internal audit, they will not satisfy requirements.

NEW QUESTION: 597
TLS provides and _____ for _____ communications.
A. Privacy, security
B. Security, optimization
C. Privacy, integrity
D. Enhancement, privacy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 598
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: (SHOW ANSWER)
Explanation
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: 599

Which of the following terms is NOT a commonly used category of risk acceptance?
A. Moderate
B. Critical
C. Minimal
D. Accepted
Answer: D (LEAVE A REPLY)
Explanation
Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

NEW QUESTION: 600
The BCDR plan/process should be written and documented in such a way that it can be used by _____.
Response:
A. Regulators
B. Essential BCDR team members
C. Users
D. Someone with the requisite skills
Answer: D (LEAVE A REPLY)

NEW QUESTION: 601
SOC Type 1 reports are considered "restricted use," in that they are intended only for limited audiences and purposes.
Which of the following is NOT a population that would be appropriate for a SOC Type 1 report?
A. Current clients
B. Auditors
C. Potential clients
D. The service organization
Answer: (SHOW ANSWER)
Explanation
Potential clients are not served by SOC Type 1 audits. A Type 2 or Type 3 report would be appropriate for potential clients. SOC Type 1 reports are intended for restricted use, where only the service organization itself, current clients, or auditors would have access to them.

NEW QUESTION: 602
Who would be responsible for implementing IPsec to secure communications for an application?
A. Developers
B. Systems staff
C. Auditors
D. Cloud customer
Answer: B (LEAVE A REPLY)
Because IPsec is implemented at the system or network level, it is the responsibility of the systems staff.
IPsec removes the responsibility from developers, whereas other technologies such as TLS would be implemented by developers.

NEW QUESTION: 603
What does SDN stand for within a cloud environment?
A. Software-dynamic networking
B. Software-defined networking
C. Software-dependent networking
D. System-dynamic nodes
Answer: B (LEAVE A REPLY)
Software-defined networking separates the administration of network filtering and network forwarding to allow for distributed administration.

NEW QUESTION: 604
What process is used within a clustered system to provide high availability and load balancing?
A. Dynamic balancing
B. Dynamic clustering
C. Dynamic optimization
D. Dynamic resource scheduling
Answer: (SHOW ANSWER)
Explanation
Dynamic resource scheduling (DRS) is used within all clustering systems as the method for clusters to provide high availability, scaling, management, and workload distribution and balancing of jobs and processes. From a physical infrastructure perspective, DRS is used to balance compute loads between physical hosts in a cloud to maintain the desired thresholds and limits on the physical hosts.

NEW QUESTION: 605
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing.
According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing?
Response:
A. Cloud customers and third parties are continually enhancing and modifying APIs.
B. APIs are a form of malware.
C. APIs can have automated settings.
D. It is impossible to uninstall APIs.
Answer: (SHOW ANSWER)

NEW QUESTION: 606
Firewalls are used to provide network security throughout an enterprise and to control what information can be accessed--and to a certain extent, through what means.
Which of the following is NOT something that firewalls are concerned with?
A. IP address
B. Encryption
C. Port
D. Protocol
Answer: (SHOW ANSWER)
Firewalls work at the network level and control traffic based on the source, destination, protocol, and ports.
Whether or not the traffic is encrypted is not a factor with firewalls and their decisions about routing traffic.
Firewalls work primarily with IP addresses, ports, and protocols.

NEW QUESTION: 607
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 (LEAVE A REPLY)
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: 608
SOC 2 reports were intended to be _____.
A. Nonbinding
B. Retained for internal use
C. Released to the public
D. Only technical assessments
Answer: (SHOW ANSWER)