ISC.CCSP.v2022-10-22.q225

Exam Code:	CCSP
Exam Name:	Certified Cloud Security Professional
Certification Provider:	ISC
Free Question Number:	225
Version:	v2022-10-22
# of views:	4007
# of Questions views:	2250
https://www.freeqas.com/qa/ISC/CCSP/ISC.CCSP.v2022-10-22.q225.html	

NEW QUESTION: 1
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)
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: 2
What does the "SOC" acronym refer to with audit reports?
A. System Organization Control
B. System Organization Confidentiality
C. Service Origin Confidentiality
D. Service Organizational Control
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Different certifications and standards take different approaches to data center design and operations. Although many traditional approaches use a tiered methodology, which of the following utilizes a macro-level approach to data center design?
A. IDCA

B. BICSI
C. Uptime Institute
D. NFPA
Answer: A (LEAVE A REPLY)
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: 4
Which of the following is not a way to manage risk?
A. Transferring
B. Accepting
C. Mitigating
D. Enveloping
Answer: (SHOW ANSWER)
Explanation
Enveloping is a nonsense term, unrelated to risk management. The rest are not.

NEW QUESTION: 5
Which of the following is the dominant driver behind the regulations to which a system or application must adhere?
A. Data source
B. Locality
C. Contract
D. SLA
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The locality--or physical location and jurisdiction where the system or data resides--is the dominant driver of regulations. This may be based on the type of data contained within the application or the way in which the data is used. The contract and SLA both articulate requirements for regulatory compliance and the responsibilities for the cloud provider and cloud customer, but neither artifact defines the actual requirements. Instead, the contract and SLA merely form the official documentation between the cloud provider and cloud customer. The source of the data may place contractual requirements or best practice guidelines on its usage, but ultimately jurisdiction has legal force and greater authority.

NEW QUESTION: 6
Which of the following threats from the OWASP Top Ten is the most difficult for an organization to protect against?
Response:
A. Denial of service
B. Advanced persistent threats
C. Account hijacking
D. Malicious insiders
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
SOX was enacted because of which of the following?
A. Poor financial controls
B. Lack of independent audits
C. All of the above
D. Poor BOD oversight
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
Who is the entity identified by personal data?
A. The data custodian
B. The data processor
C. The data subject
D. The data owner
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which of the following security technologies is commonly used to give administrators access into trust zones within an environment?
A. VPN
B. WAF
C. IPSec
D. HTTPS
Answer: A (LEAVE A REPLY)
Explanation
Virtual private networks (VPNs) are commonly used to allow access into trust zones. Via a VPN, access can be controlled and logged and only allowed through secure channels by authorized users. It also adds an additional layer of encryption and protection to communications.

NEW QUESTION: 10

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

A. Ransomware

B. Syn floods

C. XSS and SQL injection

D. Password cracking

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 11

Which concept pertains to cloud customers paying only for the resources they use and consume, and only for the duration they are using them?

A. Elasticity

B. Auto-scaling

C. Portability

D. Measured service

Answer: D (LEAVE A REPLY)

NEW QUESTION: 12

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: 13

A virtual network interface card (NIC) exists at layer _____ of the OSI model.

Response:

A. 8

B. 2

C. 6

D. 4

Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
Which of the following is NOT one of the official risk rating categories?
A. Critical
B. Low
C. Catastrophic
D. Minimal
Answer: C (LEAVE A REPLY)
The official categories of cloud risk ratings are Minimal, Low, Moderate, High, and Critical.

NEW QUESTION: 15
The different cloud service models have varying levels of responsibilities for functions and operations depending with the model's level of service.
In which of the following models would the responsibility for patching lie predominantly with the cloud customer?
A. DaaS
B. SaaS
C. PaaS
D. IaaS
Answer: (SHOW ANSWER)
With Infrastructure as a Service (IaaS), the cloud customer is responsible for deploying and maintaining its own systems and virtual machines. Therefore, the customer is solely responsible for patching and any other security updates it finds necessary. With Software as a Service (SaaS), Platform as a Service (PaaS), and Desktop as a Service (DaaS), the cloud provider maintains the infrastructure components and is responsible for maintaining and patching them.

NEW QUESTION: 16
Many aspects of cloud computing bring enormous benefits over a traditional data center, but also introduce new challenges unique to cloud computing.
Which of the following aspects of cloud computing makes appropriate data classification of high importance?
A. Multitenancy
B. Interoperability
C. Portability
D. Reversibility
Answer: A (LEAVE A REPLY)
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: 17
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: (SHOW ANSWER)
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: 18
Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality?
Response:
A. Tokenization
B. Masking
C. Anonymization
D. Obfuscation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
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: 20
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: 21
Which regulatory system pertains to the protection of healthcare data?
A. HIPAA
B. HAS
C. HITECH
D. HFCA
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:
The Health Insurance Portability and Accountability Act (HIPAA) sets stringent requirements in the United States for the protection of healthcare records.

NEW QUESTION: 22
In a Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a _____.
A. Domain name (DN)
B. Directory name (DN)
C. Distinguished name (DN)
D. Default name (DN)
Answer: (SHOW ANSWER)

NEW QUESTION: 23
The GAPP framework was developed through a joint effort between the major Canadian and American professional accounting associations in order to assist their members with managing and preventing risks to the privacy of their data and customers.
Which of the following is the meaning of GAPP?
A. General accounting privacy policies
B. Generally accepted privacy practices
C. General accounting personal privacy
D. Generally accepted privacy principles
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
Along with humidity, temperature is crucial to a data center for optimal operations and protection of equipment.
Which of the following is the optimal temperature range as set by ASHRAE?
A. 69.8 to 86.0 degrees Fahrenheit (21 to 30 degrees Celsius)
B. 51.8 to 66.2 degrees Fahrenheit (11 to 19 degrees Celsius)
C. 64.4 to 80.6 degrees Fahrenheit (18 to 27 degrees Celsius)
D. 44.6 to 60.8 degrees Fahrenheit (7 to 16 degrees Celsius)
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) recommends
64.4 to 80.6 degrees Fahrenheit (or 18 to 27 degrees Celsius) as the optimal temperature range for data centers. None of these options is the recommendation from ASHRAE.

NEW QUESTION: 25

Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality?

A. Anonymization

B. Obfuscation

C. Tokenization

D. Masking

Answer: C (LEAVE A REPLY)

NEW QUESTION: 26

What does nonrepudiation mean?

Response:

A. Prohibiting certain parties from a private conversation

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. Ensuring that a transaction is completed before saving the results

Answer: C (LEAVE A REPLY)

NEW QUESTION: 27

The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) addresses all the following security architecture elements except _____.

A. Business drivers

B. Physical security

C. IaaS

D. Application security

Answer: (SHOW ANSWER)

NEW QUESTION: 28

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)

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: 29
Which type of software is most likely to be reviewed by the most personnel, with the most varied perspectives?
Response:
A. Open source software
B. Database management software
C. Proprietary software
D. Secure software
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
Firewalls can detect attack traffic by using all these methods except _____.
Response:
A. Point of origination
B. Known past behavior in the environment
C. Identity of the malicious user
D. Signature matching
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
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: C (LEAVE A REPLY)
Explanation/Reference:
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: 32
You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Previous releases have shipped with major flaws that were not detected in the testing phase; leadership wants to avoid repeating that problem.
What tool/technique/technology might you suggest to aid in identifying programming errors?
A. Vulnerability scans
B. Regulatory review
C. SOC audits
D. Open source review
Answer: D (LEAVE A REPLY)

NEW QUESTION: 33
Which data protection strategy would be useful for a situation where the ability to remove sensitive data from a set is needed, but a requirement to retain the ability to map back to the original values is also present?
A. Masking
B. Tokenization
C. Encryption
D. Anonymization
Answer: B (LEAVE A REPLY)
Tokenization involves the replacement of sensitive data fields with key or token values, which can ultimately be mapped back to the original, sensitive data values. Masking refers to the overall approach to covering sensitive data, and anonymization is a type of masking, where indirect identifiers are removed from a data set to prevent the mapping back of data to an individual. Encryption refers to the overall process of protecting data via key pairs and protecting confidentiality.

NEW QUESTION: 34
Which audit type has been largely replaced by newer approaches since 2011?
A. SOC Type 1
B. SSAE-16

C. SAS-70
D. SOC Type 2
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
SAS-70 reports were replaced in 2011 with the SSAE-16 reports throughout the industry.

NEW QUESTION: 35
Which value refers to the percentage of production level restoration needed to meet BCDR objectives?
A. RPO
B. RTO
C. RSL
D. SRE
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The recovery service level (RSL) is a percentage measure of the total typical production service level that needs to be restored to meet BCDR objectives in the case of a failure.

NEW QUESTION: 36
Firewalls are used to provide network security throughout an enterprise and to control what information can be accessed--and to a certain extent, through what means.
Which of the following is NOT something that firewalls are concerned with?
A. IP address
B. Encryption
C. Port
D. Protocol
Answer: B (LEAVE A REPLY)
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: 37
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: 38
Which of the following is NOT a key area for performance monitoring as far as an SLA is concerned?
A. CPU
B. Users
C. Memory
D. Network
Answer: (SHOW ANSWER)
Explanation
An SLA requires performance monitoring of CPU, memory, storage, and networking. The number of users active on a system would not be part of an SLA specifically, other than in regard to the impact on the other four variables.

NEW QUESTION: 39
You just hired an outside developer to modernize some applications with new web services and functionality. In order to implement a comprehensive test platform for validation, the developer needs a data set that resembles a production data set in both size and composition.
In order to accomplish this, what type of masking would you use?
A. Development
B. Replicated
C. Static
D. Dynamic
Answer: (SHOW ANSWER)
Static masking takes a data set and produces a copy of it, but with sensitive data fields masked. This allows for a full data set from production for testing purposes, but without any sensitive data. Dynamic masking works with a live system and is not used to produce a distinct copy. The terms "replicated" and "development" are not types of masking.

NEW QUESTION: 40
Halon is now illegal to use for data center fire suppression. What is the reason it was outlawed?
A. It does not adequately suppress fires.

B. It causes undue damage to electronic systems.
C. It can harm the environment.
D. It poses a threat to health and human safety when deployed.
Answer: (SHOW ANSWER)

NEW QUESTION: 41
A truly airgapped machine selector will _____.
Response:
A. Not be portable
B. Terminate a connection before creating a new connection
C. Be made of composites and not metal
D. Have total Faraday properties
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
Aside from the fact that the cloud customer probably cannot locate/reach the physical storage assets of the cloud provider, and that wiping an entire storage space would impact other customers, why would degaussing probably not be an effective means of secure sanitization in the cloud?
Response:
A. Cloud data storage may not be affected by degaussing.
B. The blast radius is too wide.
C. Federal law prohibits it in the United States.
D. All the data storage space in the cloud is already gaussed.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 43
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:
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: 44

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: 45
A crucial decision any company must make is in regard to where it hosts the data systems it depends on. A debate exists as to whether it's best to lease space in a data center or build your own data center--and now with cloud computing, whether to purchase resources within a cloud.
What is the biggest advantage to leasing space in a data center versus procuring cloud services?
A. Regulations
B. Control
C. Security
D. Costs
Answer: B (LEAVE A REPLY)
Explanation
When leasing space in a data center versus utilizing cloud services, a customer has a much greater control over its systems and services, from both the hardware/software perspective and the operational management perspective. Costs, regulations, and security are all prime considerations regardless of the hosting type selected. Although regulations will be the same in either hosting solution, in most instances, costs and security will be greater factors with leased space.

NEW QUESTION: 46
DLP solutions can aid in deterring loss due to which of the following?
A. Device failure
B. Randomization
C. Inadvertent disclosure
D. Natural disaster
Answer: C (LEAVE A REPLY)
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: 47
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: 48
Which network protocol is essential for allowing automation and orchestration within a cloud environment?
Response:
A. VLANs
B. IPsec
C. DHCP
D. DNSSEC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
User access to the cloud environment can be administered in all of the following ways except:
A. Provider provides administration on behalf the customer
B. Customer directly administers access
C. Third party provides administration on behalf of the customer
D. Customer provides administration on behalf of the provider
Answer: D (LEAVE A REPLY)
Explanation/Reference:

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

NEW QUESTION: 50
Which of the following technologies is NOT commonly used for accessing systems and services in a cloud environment in a secure manner?
A. KVM
B. HTTPS
C. VPN
D. TLS
Answer: A (LEAVE A REPLY)
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: 51
The cloud deployment model that features joint ownership of assets among an affinity group is known as:
A. Private
B. Public
C. Community
D. Hybrid
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52
The most pragmatic option for data disposal in the cloud is which of the following?
A. Cryptoshredding
B. Overwriting
C. Cold fusion
D. Melting
Answer: A (LEAVE A REPLY)
We don't have physical ownership, control, or even access to the devices holding the data, so physical destruction, including melting, is not an option. Overwriting is a possibility, but it is complicated by the difficulty of locating all the sectors and storage areas that might have contained our data, and by the likelihood that constant backups in the cloud increase the

chance we'll miss something as it's being overwritten. Cryptoshredding is the only reasonable alternative.
Cold fusion is a red herring.

NEW QUESTION: 53
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: (SHOW ANSWER)
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: 54
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)
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: 55
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: 56
If you're using iSCSI in a cloud environment, what must come from an external protocol or application?
A. Kerberos support
B. CHAP support
C. Authentication
D. Encryption
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
iSCSI does not natively support encryption, so another technology such as IPsec must be used to encrypt communications.

NEW QUESTION: 57
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
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: 58
A federated identity system is composed of three main components. Which of the following is NOT one of the three main components?
A. Identity provider
B. User

C. API
D. Relying party
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
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: 60
What is a form of cloud storage where data is stored as objects, arranged in a hierarchal structure, like a file tree?
A. Volume storage
B. Databases
C. Content delivery network (CDN)
D. Object storage
Answer: (SHOW ANSWER)

NEW QUESTION: 61
The physical layout of a cloud data center campus should include redundancies of all the following except _____.
Response:
A. Electrical utility lines
B. Communications connectivity lines
C. The administration/support staff building
D. Physical perimeter security controls (fences, lights, walls, etc.)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 62
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)
Explanation
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: 63
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. Private
D. Public
Answer: C (LEAVE A REPLY)

NEW QUESTION: 64
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)
Explanation/Reference:

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

NEW QUESTION: 65
Which of the following statements best describes a Type 1 hypervisor?
A. The hypervisor software runs within an operating system tied to the hardware.
B. The hypervisor software runs as a client on a server and needs an external service to administer it.
C. The hypervisor software runs on top of an application layer.
D. The hypervisor software runs directly on "bare metal" without an intermediary.
Answer: D (LEAVE A REPLY)
With a Type 1 hypervisor, the hypervisor software runs directly on top of the bare-metal system, without any intermediary layer or hosting system. None of these statements describes a Type 1 hypervisor.

NEW QUESTION: 66
Although encryption can help an organization to effectively decrease the possibility of data breaches, which other type of threat can it increase the chances of?
A. Data loss
B. Insecure interfaces
C. Account hijacking
D. System vulnerabilities
Answer: A (LEAVE A REPLY)

NEW QUESTION: 67
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
The SOAP protocol only supports the XML data format.

NEW QUESTION: 68
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)
Explanation
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: 69
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: (SHOW ANSWER)
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: 70
What is the risk to the organization posed by dashboards that display data discovery results?
Response:
A. Flawed management decisions based on massaged displays
B. Higher likelihood of inadvertent disclosure
C. Raised incidence of physical theft
D. Increased chance of external penetration
Answer: (SHOW ANSWER)

NEW QUESTION: 71
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)
Explanation/Reference:
Explanation:
The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated services. A cloud service administrator is responsible for testing, monitoring, and securing cloud services, as well as providing usage reporting and dealing with service problems. The cloud service integrator is responsible for connecting existing systems and services with a cloud. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

NEW QUESTION: 72
All of the following are techniques to enhance the portability of cloud data, in order to minimize the potential of vendor lock-in except:
A. Ensure there are no physical limitations to moving
B. Use DRM and DLP solutions widely throughout the cloud operation
C. Ensure favorable contract terms to support portability
D. Avoid proprietary data formats
Answer: (SHOW ANSWER)
Explanation
DRM and DLP are used for increased authentication/access control and egress monitoring, respectively, and would actually decrease portability instead of enhancing it.

NEW QUESTION: 73
A data custodian is responsible for which of the following?
A. Data context
B. Data content
C. The safe custody, transport, storage of the data, and implementation of business rules
D. Logging access and alerts
Answer: (SHOW ANSWER)
A data custodian is responsible for the safe custody, transport, and storage of data, and the implementation of business roles.

NEW QUESTION: 74
What are third-party providers of IAM functions for the cloud environment?
A. CASBs
B. DLPs
C. SIEMs
D. AESs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
Limits for resource utilization can be set at different levels within a cloud environment to ensure that no particular entity can consume a level of resources that impacts other cloud customers.
Which of the following is NOT a unit covered by limits?
A. Hypervisor
B. Cloud customer
C. Virtual machine
D. Service
Answer: A (LEAVE A REPLY)
Explanation
The hypervisor level, as a backend cloud infrastructure component, is not a unit where limits may be applied to control resource utilization. Limits can be placed at the service, virtual machine, and cloud customer levels within a cloud environment.

NEW QUESTION: 76
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: 77

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)

Explanation/Reference:

Explanation:

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

NEW QUESTION: 78

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)

Explanation/Reference:

Explanation:

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: 79

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: (SHOW ANSWER)
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: 80
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Background checks are controls for attenuating potential threats from internal actors; external threats aren't likely to submit to background checks.

NEW QUESTION: 81
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: 82
What is the amount of fuel that should be on hand to power generators for backup datacenter power, in all tiers, according to the Uptime Institute?
A. 1

B. 12 hours
C. As much as needed to ensure all systems may be gracefully shut down and data securely stored
D. 1,000 gallons
Answer: B (LEAVE A REPLY)

NEW QUESTION: 83
Gathering business requirements can aid the organization in determining all of this information about organizational assets, except:
A. Full inventory
B. Criticality
C. Value
D. Usefulness
Answer: (SHOW ANSWER)
When we gather information about business requirements, we need to do a complete inventory, receive accurate valuation of assets (usually from the owners of those assets), and assess criticality; this collection of information does not tell us, objectively, how useful an asset is, however.

NEW QUESTION: 84
The physical layout of a cloud data center campus should include redundancies of all the following except _____.
A. HVAC units
B. Generator fuel storage
C. Generators
D. Points of personnel ingress
Answer: D (LEAVE A REPLY)

NEW QUESTION: 85
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: 86

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: 87

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: 88

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)

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: 89

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

A. Confidentiality

B. Portability

C. Availability

D. Integrity

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 90

All of these are reasons an organization may want to consider cloud migration except:

Response:

A. Reduced operational expenses

B. Reduced personnel costs

C. Elimination of risks

D. Increased efficiency

Answer: C (LEAVE A REPLY)

NEW QUESTION: 91

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: (SHOW ANSWER)

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: 92
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 "sensitive data exposure." Which of these is a technique to reduce the potential for a sensitive data exposure?
Response:
A. Roving security guards
B. Extensive user training on proper data handling techniques
C. Ensuring the use of utility backup power supplies
D. Advanced firewalls inspecting all inbound traffic, to include content-based screening
Answer: (SHOW ANSWER)

NEW QUESTION: 93
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 get truly holistic coverage of your environment, you should be sure to include _____ as a step in the deployment process.
Response:
A. All of your customers to install the tool
B. Installation of the solution on all assets in the cloud data center
C. Adoption of the tool in all routers between your users and the cloud provider
D. Getting signed user agreements from all users
Answer: D (LEAVE A REPLY)

NEW QUESTION: 94
Which component of ITIL involves planning for the restoration of services after an unexpected outage or incident?
A. Continuity management
B. Problem management
C. Configuration management
D. Availability management
Answer: (SHOW ANSWER)
Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur. Availability management is focused on making sure

system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Configuration management tracks and maintains detailed information about all IT components within an organization.

NEW QUESTION: 95
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. Credential
B. Certificate
C. Ticket
D. Token
Answer: D (LEAVE A REPLY)

NEW QUESTION: 96
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/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: 97
Which data state would be most likely to use TLS as a protection mechanism?
A. Data in use
B. Data at rest
C. Archived
D. Data in transit
Answer: D (LEAVE A REPLY)
TLS would be used with data in transit, when packets are exchanged between clients or services and sent across a network. During the data-in-use state, the data is already protected via a technology such as TLS as it is exchanged over the network and then relies on other technologies such as digital signatures for protection while being used. The data-at-rest state primarily uses encryption for stored file objects.
Archived data would be the same as data at rest.

NEW QUESTION: 98
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
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: 99
From a security perspective, which of the following is a major concern when evaluating possible BCDR solutions?
A. Access provisioning
B. Auditing
C. Jurisdictions
D. Authorization
Answer: C (LEAVE A REPLY)
When a security professional is considering cloud solutions for BCDR, a top concern is the jurisdiction where the cloud systems are hosted. If the jurisdiction is different from where the production systems are hosted, they may be subjected to different regulations and controls, which would make a seamless BCDR solution far more difficult.

NEW QUESTION: 100
What type of security threat is DNSSEC designed to prevent?
A. Account hijacking
B. Snooping
C. Spoofing
D. Injection
Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 101
A cloud data encryption situation where the cloud customer retains control of the encryption keys and the cloud provider only processes and stores the data could be considered a _____.
Response:
A. Case of infringing on the rights of the provider
B. Threat
C. Risk
D. Hybrid cloud deployment model
Answer: D (LEAVE A REPLY)

NEW QUESTION: 102
Which of the following is a risk that stems from a virtualized environment?
Response:
A. It is difficult to find and contract with multiple utility providers of the same type (electric, water, etc.).
B. Cloud data centers can become a single point of failure.
C. Modern SLA demands are stringent and very hard to meet.
D. Live virtual machines in the production environment are moved from one host to another in the clear.
Answer: (SHOW ANSWER)

NEW QUESTION: 103
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: (SHOW ANSWER)
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: 104

DLP solutions can aid all of the following security-related efforts except _____.
Response:
A. Egress monitoring
B. Access control
C. e-discovery/forensics
D. Data categorization/classification
Answer: B (LEAVE A REPLY)

NEW QUESTION: 105
Deviations from the baseline should be investigated and _____.
A. Revealed
B. Documented
C. Encouraged
D. Enforced
Answer: (SHOW ANSWER)
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: 106
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)
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: 107
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)
Explanation
Data that falls under the purview of an eDiscovery request is that which is in the possession, custody, or control of the organization. Although this is an easy concept in a traditional data center, it can be difficult to distinguish who actually possesses and controls the data in a cloud environment due to multitenancy and resource pooling. Although these options provide similar-sounding terms, they are ultimately incorrect.

NEW QUESTION: 108
Which data state would be most likely to use TLS as a protection mechanism?
A. Data in use
B. Data at rest
C. Archived
D. Data in transit
Answer: D (LEAVE A REPLY)
Explanation
TLS would be used with data in transit, when packets are exchanged between clients or services and sent across a network. During the data-in-use state, the data is already protected via a technology such as TLS as it is exchanged over the network and then relies on other technologies such as digital signatures for protection while being used. The data-at-rest state primarily uses encryption for stored file objects. Archived data would be the same as data at rest.

NEW QUESTION: 109
Which of the following is considered an administrative control?
A. Keystroke logging
B. Access control process

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

NEW QUESTION: 110
Security is a critical yet often overlooked consideration for BCDR planning.
At which stage of the planning process should security be involved?
A. Scope definition
B. Requirements gathering
C. Analysis
D. Risk assessment
Answer: A (LEAVE A REPLY)
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: 111
Which of the following terms is not associated with cloud forensics?
A. eDiscovery
B. Chain of custody
C. Analysis
D. Plausibility
Answer: (SHOW ANSWER)
Explanation
Plausibility, here, is a distractor and not specifically relevant to cloud forensics.

NEW QUESTION: 112
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: 113
All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline, except _____.
A. Audit the baseline to ensure that all configuration items have been included and applied correctly
B. Document all baseline configuration elements and versioning data
C. Capture an image of the baseline system for future reference/versioning/rollback purposes
D. Impose the baseline throughout the environment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 114
What does a cloud customer purchase or obtain from a cloud provider?
A. Services
B. Hosting
C. Servers
D. Customers
Answer: A (LEAVE A REPLY)
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: 115
Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like:
A. Ransomware
B. Syn floods
C. XSS and SQL injection
D. Password cracking
Answer: (SHOW ANSWER)
Explanation

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

NEW QUESTION: 116
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: 117
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: 118
Which of the following cloud aspects complicates eDiscovery?
A. Resource pooling
B. On-demand self-service
C. Multitenancy

D. Measured service
Answer: (SHOW ANSWER)
Explanation
Explanation:
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: 119
Which of the following are attributes of cloud computing?
A. Minimal management effort and shared resources
B. High cost and unique resources
C. Rapid provisioning and slow release of resources
D. Limited access and service provider interaction
Answer: (SHOW ANSWER)
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NEW QUESTION: 120
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: 121
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: 122

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)

Explanation

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: 123

You are the security policy lead for your organization, which is considering migrating from your on- premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization. What is probably the best benefit offered by the CCM?

A. The low cost of the tool

B. Simplicity of control selection from the list of approved choices

C. Allowing your organization to leverage existing controls across multiple frameworks so as not to duplicate effort
D. Ease of implementation by choosing controls from the list of qualified vendors
Answer: C (LEAVE A REPLY)

NEW QUESTION: 124
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: 125
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: 126
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

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: 127
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)
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: 128
What is the term used to describe loss of access to data because the cloud provider has ceased operation?
Response:
A. Masking
B. Vendor lock-in
C. Closing
D. Vendor lock-out
Answer: D (LEAVE A REPLY)

NEW QUESTION: 129
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
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: 130
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
What should you not expect the tool to address?
A. Sensitive data sent inadvertently in user emails
B. Sensitive data captured by screen shots
C. Sensitive data moved to external devices
D. Sensitive data in the contents of files sent via FTP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 131
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
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: 132
The share phase of the cloud data lifecycle involves allowing data to leave the application, to be shared with external systems, services, or even other vendors/contractors.
What technology would be useful for protecting data at this point?
A. IDS
B. DLP
C. IPS
D. WAF
Answer: B (LEAVE A REPLY)
Data loss prevention (DLP) solutions allow for control of data outside of the application or original system.
They can enforce granular control such as printing, copying, and being read by others, as well as forcing expiration of access. Intrusion detection system (IDS) and intrusion

prevention system (IPS) solutions are used for detecting and blocking suspicious and malicious traffic, respectively, whereas a web application firewall (WAF) is used for enforcing security or other controls on web- based applications.

NEW QUESTION: 133
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 _____.
Response:
A. Cloud enhancement
B. Cloud bursting
C. Cloud fragility
D. Cloud framing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 134
You need to gain approval to begin moving your company's data and systems into a cloud environment.
However, your CEO has mandated the ability to easily remove your IT assets from the cloud provider as a precondition.
Which of the following cloud concepts would this pertain to?
A. Removability
B. Extraction
C. Portability
D. Reversibility
Answer: D (LEAVE A REPLY)
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: 135
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 "security misconfiguration." Which of these is a technique to reduce the potential for a security misconfiguration?
Response:
A. Perform periodic scans and audits of the environment.
B. Get regulatory approval for major configuration modifications.
C. Update the BCDR plan on a timely basis.
D. Train all users on proper security procedures.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 136
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 poses a threat to health and human safety when deployed.
C. It can harm the environment.
D. It does not adequately suppress fires.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 137
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)
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: 138

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)
Explanation
The physical security of crypto keys is of some concern, but guards or vaults are not always necessary.
Two-person integrity might be a good practice for protecting keys. The best answer to this question is option A, because it is always true, whereas the remaining options depend on circumstances.

NEW QUESTION: 139
_____ can often be the result of inadvertent activity.
Response:
A. Disasters
B. DDoS
C. Phishing
D. Sprawl
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
With software-defined networking, what aspect of networking is abstracted from the forwarding of traffic?
A. Routing
B. Session
C. Filtering
D. Firewalling
Answer: C (LEAVE A REPLY)
Explanation
With software-defined networking (SDN), the filtering of network traffic is separated from the forwarding of network traffic so that it can be independently administered.

NEW QUESTION: 141
Typically, SSDs are _____.
Response:
A. Heavier than tape libraries
B. Larger than tape backup
C. More subject to malware than legacy drives
D. More expensive than spinning platters

Answer: (SHOW ANSWER)

NEW QUESTION: 142
There are many situations when testing a BCDR plan is appropriate or mandated.
Which of the following would not be a necessary time to test a BCDR plan?
A. After software updates
B. After regulatory changes
C. After major configuration changes
D. Annually
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Regulatory changes by themselves would not trigger a need for new testing of a BCDR plan. Any changes necessary for regulatory compliance would be accomplished through configuration changes or software updates, which in turn would then trigger the necessary new testing. Annual testing is crucial to any BCDR plan. Also, any time major configuration changes or software updates are done, the plan should be evaluated and tested to ensure it is still valid and complete.

NEW QUESTION: 143
Which of the following is a method for apportioning resources that involves setting maximum usage amounts for all tenants/customers within the environment?
A. Shares
B. Reservations
C. Cancellations
D. Limits
Answer: D (LEAVE A REPLY)

NEW QUESTION: 144
What must SOAP rely on for security?
A. Encryption
B. Tokenization
C. TLS
D. SSL
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
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: 145

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)
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: 146
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: B (LEAVE A REPLY)
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: 147
If you are running an application that has strict legal requirements that the data cannot reside on systems that contain other applications or systems, which aspect of cloud computing would be prohibitive in this case?
A. Multitenancy
B. Broad network access
C. Portability
D. Elasticity
Answer: A (LEAVE A REPLY)
Explanation
Multitenancy is the aspect of cloud computing that involves having multiple customers and applications running within the same system and sharing the same resources. Although considerable mechanisms are in place to ensure isolation and separation, the data and applications are ultimately using shared resources. Broad network access refers to the ability to access cloud services from any location or client. Portability refers to the ability to easily move cloud services between different cloud providers, whereas elasticity refers to the capabilities of a cloud environment to add or remove services, as needed, to meet current demand.

NEW QUESTION: 148
What type of PII is regulated based on the type of application or per the conditions of the specific hosting agreement?
A. Specific
B. Contractual
C. regulated
D. Jurisdictional
Answer: B (LEAVE A REPLY)
Contractual PII has specific requirements for the handling of sensitive and personal information, as defined at a contractual level. These specific requirements will typically document the required handling procedures and policies to deal with PII. They may be in specific security controls and configurations, required policies or procedures, or limitations on who may gain authorized access to data and systems.

NEW QUESTION: 149
Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?
A. SOC 1
B. SOC 2
C. SOC 3
D. SOC 4
Answer: (SHOW ANSWER)
SOC 2 deals with the CIA triad. SOC 1 is for financial reporting. SOC 3 is only an attestation by the auditor. There is no SOC 4.

NEW QUESTION: 150
Database activity monitoring (DAM) can be:
A. Host-based or network-based
B. Server-based or client-based
C. Used in the place of encryption
D. Used in place of data masking
Answer: A (LEAVE A REPLY)
We don't use DAM in place of encryption or masking; DAM augments these options without replacing them. We don't usually think of the database interaction as client-server, so A is the best answer.

NEW QUESTION: 151
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: 152
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: (SHOW ANSWER)
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: 153
Which of the following is a risk associated with manual patching especially in the cloud?
Response:
A. Lack of applicability to the environment
B. No notice before the impact is realized
C. Patches may or may not address the vulnerability they were designed to fix.
D. The possibility for human error
Answer: D (LEAVE A REPLY)

NEW QUESTION: 154
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: (SHOW ANSWER)
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: 155
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: 156
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: 157
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: 158
Because of multitenancy, specific risks in the public cloud that don't exist in the other cloud service models include all the following except:
A. DoS/DDoS
B. Information bleed
C. Risk of loss/disclosure due to legal seizures
D. Escalation of privilege
Answer: (SHOW ANSWER)
Explanation
DoS/DDoS threats and risks are not unique to the public cloud model.

NEW QUESTION: 159
A bare-metal hypervisor is Type _____.
A. 1
B. 3
C. 2
D. 4
Answer: (SHOW ANSWER)

NEW QUESTION: 160
Which entity requires all collection and storing of data on their citizens to be done on hardware that resides within their borders?
A. Russia
B. France
C. Germany
D. United States

Answer: (SHOW ANSWER)
Signed into law and effective starting on September 1, 2015, Russian Law 526-FZ establishes that any collecting, storing, or processing of personal information or data on Russian citizens must be done from systems and databases that are physically located with the Russian Federation.

NEW QUESTION: 161
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: 162
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: (SHOW ANSWER)
Explanation
The most common and efficient manner of securing operating systems is through the use of baselines. A baseline is a standardized and understood set of base configurations and settings. When a new system is built or a new virtual machine is established, baselines will be applied to a new image to ensure the base configuration meets organizational policy and regulatory requirements.

NEW QUESTION: 163
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: 164

You are working for a cloud service provider and receive an eDiscovery order pertaining to one of your customers.

Which of the following would be the most appropriate action to take first?

A. Take a shapshot of the virtual machines

B. Escrow the encryption keys

C. Copy the data

D. Notify the customer

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

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

NEW QUESTION: 165

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

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

A. SOC 2

B. SAS-70

C. SOC 3

D. SOC 1

Answer: (SHOW ANSWER)

Explanation

SOC Type 3 audit reports are very similar to SOC Type 2, with the exception that they are intended for general release and public audiences.SAS-70 audits have been deprecated.

SOC Type 1 audit reports have a narrow scope and are intended for very limited release,

whereas SOC Type 2 audit reports are intended for wider audiences but not general release.

NEW QUESTION: 166
What does the management plane typically utilize to perform administrative functions on the hypervisors that it has access to?
A. Scripts
B. RDP
C. APIs
D. XML
Answer: C (LEAVE A REPLY)
The functions of the management plane are typically exposed as a series of remote calls and function executions and as a set of APIs. These APIs are typically leveraged through either a client or a web portal, with the latter being the most common.

NEW QUESTION: 167
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/Reference:
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: 168

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

NEW QUESTION: 169
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)?
A. Fines
B. Jail time
C. Subject to increased audit frequency and scope
D. Suspension of credit card processing privileges
Answer: (SHOW ANSWER)

NEW QUESTION: 170
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)
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: 171
The goals of SIEM solution implementation include all of the following, except:
A. Dashboarding
B. Performance enhancement
C. Trend analysis
D. Centralization of log streams
Answer: B (LEAVE A REPLY)
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: 172
What masking strategy involves the replacing of sensitive data at the time it is accessed and used as it flows between the data and application layers of a service?
A. Active
B. Static
C. Dynamic
D. Transactional
Answer: C (LEAVE A REPLY)
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: 173
In a federated identity arrangement using a trusted third-party model, who is the identity provider and who is the relying party?
A. The users of the various organizations within the federations within the federation/a CASB
B. Each member organization/a trusted third party
C. Each member organization/each member organization
D. A contracted third party/the various member organizations of the federation
Answer: (SHOW ANSWER)
In a trusted third-party model of federation, each member organization outsources the review and approval task to a third party they all trust. This makes the third party the identifier (it issues and manages identities for all users in all organizations in the federation), and the various member organizations are the relying parties (the resource providers that share resources based on approval from the third party).

NEW QUESTION: 174
Which of the following is the best example of a key component of regulated PII?
Response:
A. PCI DSS
B. Mandatory breach reporting
C. Items that should be implemented
D. Audit rights of subcontractors
Answer: (SHOW ANSWER)

NEW QUESTION: 175
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: 176
Which of the following is considered a physical control?
A. Fences
B. Ceilings
C. Carpets
D. Doors
Answer: A (LEAVE A REPLY)
Explanation
Fences are physical controls; carpets and ceilings are architectural features, and a door is not necessarily a control: the lock on the door would be a physical security control. Although you might think of a door as a potential answer, the best answer is the fence; the exam will have questions where more than one answer is correct, and the answer that will score you points is the one that is most correct.

NEW QUESTION: 177
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: 178
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: (SHOW ANSWER)
The guidelines from ASHRAE establish 64.4-80.6degF (18-27degC) as the optimal temperature for a data center.

NEW QUESTION: 179
Implementing baselines on systems would take an enormous amount of time and resources if the staff had to apply them to each server, and over time, it would be almost impossible to keep all the systems in sync on an ongoing basis.
Which of the following is NOT a package that can be used for implementing and maintaining baselines across an enterprise?
A. Puppet
B. SCCM
C. Chef
D. GitHub
Answer: D (LEAVE A REPLY)
GitHub is a software development platform that serves as a code repository and versioning system. It is solely used for software development and would not be appropriate for applying baselines to systems. Puppet is an open-source configuration management tool that runs on many platforms and can be used to apply and maintain baselines. The Software Center Configuration Manager (SCCM) was developed by Microsoft for

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

NEW QUESTION: 180
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: (SHOW ANSWER)
Explanation
Structured storage involves organized and categorized data, which most closely resembles and operates like a database system would.

NEW QUESTION: 181
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: (SHOW ANSWER)
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: 182
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: 183
Deviations from the baseline should be investigated and _____.
A. Revealed
B. Documented
C. Encouraged
D. Enforced
Answer: B (LEAVE A REPLY)
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: 184
The BIA can be used to provide information about all the following, except:

A. BC/DR planning
B. Risk analysis
C. Secure acquisition
D. Selection of security controls
Answer: (SHOW ANSWER)
Explanation
The business impact analysis gathers asset valuation information that is beneficial for risk analysis and selection of security controls (it helps avoid putting the ten-dollar lock on the five-dollar bicycle), and criticality information that helps in BC/DR planning by letting the organization understand which systems, data, and personnel are necessary to continuously maintain. However, it does not aid secure acquisition efforts, since the assets examined by the BIA have already been acquired.

NEW QUESTION: 185
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)
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 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: 186
The SOC Type 2 reports are divided into five principles.
Which of the five principles must also be included when auditing any of the other four principles?
A. Confidentiality
B. Privacy
C. Security
D. Availability
Answer: C (LEAVE A REPLY)
Explanation

Explanation:
Under the SOC guidelines, when any of the four principles other than security are being audited, which includes availability, confidentiality, processing integrity, and privacy, the security principle must also be included with the audit.

NEW QUESTION: 187
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: 188
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: (SHOW ANSWER)
Explanation
The SOC 3 is the least detailed, so the provider is not concerned about revealing it. The SOC 1 Types 1 and 2 are about financial reporting, and not relevant. The SOC 2 Type 2 is much more detailed and will most likely be kept closely held by the provider.

NEW QUESTION: 189
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. Reservations
B. Resource pooling
C. Limits
D. Shares
Answer: A (LEAVE A REPLY)

NEW QUESTION: 190
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: 191
What are SOCI/SOCII/SOCIII?
A. Risk management frameworks
B. Software development phases
C. Audit reports
D. Access controls
Answer: (SHOW ANSWER)

NEW QUESTION: 192
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?
Response:
A. PKI certificates
B. Multifactor authentication
C. Preexisting knowledge of each other
D. Out-of-band authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 193
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 _____.
A. The amount of product the plant creates
B. The length of time it would take to rebuild the plant
C. The amount of revenue generated by the plant
D. The rate at which the plant generates revenue
Answer: A (LEAVE A REPLY)

NEW QUESTION: 194
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: (SHOW ANSWER)
Explanation
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: 195
Static software security testing typically uses _____ as a measure of how thorough the testing was.
A. Number of testers
B. Flaws detected

C. Malware hits
D. Code coverage
Answer: D (LEAVE A REPLY)

NEW QUESTION: 196
The BCDR plan/process should be written and documented in such a way that it can be used by _____.
Response:
A. Someone with the requisite skills
B. Regulators
C. Users
D. Essential BCDR team members
Answer: (SHOW ANSWER)

NEW QUESTION: 197
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: A (LEAVE A REPLY)
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: 198
The cloud deployment model that features organizational ownership of the hardware and infrastructure, and usage only by members of that organization, is known as:
Response:
A. Hybrid
B. Motive
C. Private
D. Public
Answer: (SHOW ANSWER)

NEW QUESTION: 199
You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment.
Management is interested in adopting an Agile development style.
This will be typified by which of the following traits?
Response:
A. Rigorous, repeated security testing
B. Isolated programming experts for specific functional elements
C. Reliance on a concrete plan formulated during the Define phase
D. Short, iterative work periods
Answer: D (LEAVE A REPLY)

NEW QUESTION: 200
With software-defined networking, what aspect of networking is abstracted from the forwarding of traffic?
A. Routing
B. Session
C. Filtering
D. Firewalling
Answer: C (LEAVE A REPLY)
With software-defined networking (SDN), the filtering of network traffic is separated from the forwarding of network traffic so that it can be independently administered.

NEW QUESTION: 201
Which type of software is most likely to be reviewed by the most personnel, with the most varied perspectives?
A. Database management software
B. Proprietary software

C. Secure software
D. Open source software
Answer: D (LEAVE A REPLY)

NEW QUESTION: 202
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/Reference:
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: 203
Which of the following is considered a physical control?
A. Fences
B. Ceilings
C. Carpets
D. Doors
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:

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

NEW QUESTION: 204
Why does the physical location of your data backup and/or BCDR failover environment matter?
A. Environmental factors such as humidity
B. It may affect regulatory compliance
C. Lack of physical security
D. It doesn't matter. Data can be saved anywhere without consequence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 205
Which of the following is the dominant driver behind the regulations to which a system or application must adhere?
A. Data source
B. Locality
C. Contract
D. SLA
Answer: B (LEAVE A REPLY)
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: 206
A loosely coupled storage cluster will have performance and capacity limitations based on the
_____.
Response:
A. Physical backplane connecting it
B. The performance and capacity in each node
C. Total number of nodes in the cluster
D. Amount of usage demanded

Answer: B (LEAVE A REPLY)

NEW QUESTION: 207
IRM solutions allow an organization to place different restrictions on data usage than would otherwise be possible through traditional security controls.
Which of the following controls would be possible with IRM that would not with traditional security controls?
A. Copy
B. Read
C. Delete
D. Print
Answer: D (LEAVE A REPLY)
Traditional security controls would not be able to restrict a user from printing something that they have the ability to access and read, but IRM solutions would allow for such a restriction. If a user has permissions to read a file, he can also copy the file or print it under traditional controls, and the ability to modify or write will give the user the ability to delete.

NEW QUESTION: 208
Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?
A. Unvalidated redirects and forwards
B. Cross-site request forgery
C. Cross-site scripting
D. Insecure direct object references
Answer: (SHOW ANSWER)

NEW QUESTION: 209
Which ITIL component is an ongoing, iterative process of tracking all deployed and configured resources that an organization uses and depends on, whether they are hosted in a traditional data center or a cloud?
A. Problem management
B. Continuity management
C. Availability management
D. Configuration management
Answer: (SHOW ANSWER)
Explanation
Configuration management tracks and maintains detailed information about all IT components within an organization. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an

unexpected outage, incident, or disaster. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION: 210
Which security certification serves as a general framework that can be applied to any type of system or application?
A. FIPS 140-2
B. PCI DSS
C. ISO/IEC 27001
D. NIST SP 800-53
Answer: C (LEAVE A REPLY)

NEW QUESTION: 211
All of these are methods of data discovery, except:
A. Label-based
B. User-based
C. Content-based
D. Metadata-based
Answer: B (LEAVE A REPLY)
Explanation
All the others are valid methods of data discovery; user-based is a red herring with no meaning.

NEW QUESTION: 212
A honeypot should contain _____ data.
A. Sensitive
B. Useless
C. Production
D. Raw
Answer: (SHOW ANSWER)

NEW QUESTION: 213

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. Anonymization
B. Obfuscation
C. Masking
D. Encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 214
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: 215
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. Malware
D. DoS/DDoS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 216
What type of data does data rights management (DRM) protect?
A. Consumer
B. PII
C. Financial
D. Healthcare

Answer: A (LEAVE A REPLY)
DRM applies to the protection of consumer media, such as music, publications, video, movies, and soon.

NEW QUESTION: 217
Which of the following BCDR testing methodologies is least intrusive?
Response:
A. Full test
B. Walk-through
C. Tabletop
D. Simulation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 218
Which of the following concepts refers to a cloud customer paying only for the resources and offerings they use within a cloud environment, and only for the duration that they are consuming them?
A. Consumable service
B. Measured service
C. Billable service
D. Metered service
Answer: B (LEAVE A REPLY)
Explanation
Measured service is where cloud services are delivered and billed in a metered way, where the cloud customer only pays for those that they actually use, and for the duration of time that they use them.

NEW QUESTION: 219
Patches do all the following except _____.
Response:
A. Solve cloud interoperability problems
B. Address performance issues
C. Add new features and capabilities to existing systems
D. Address newly discovered vulnerabilities
Answer: A (LEAVE A REPLY)

NEW QUESTION: 220
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: 221
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)
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: 222
Software-defined networking (SDN) is intended to separate different network capabilities and allow for the granting of granular configurations, permissions, and features to non-network staff or customers. Which network capability is separated from forwarding of traffic?
Response:
A. Firewalling
B. Filtering
C. Routing
D. IPS
Answer: (SHOW ANSWER)

NEW QUESTION: 223
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: 224
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. Insecure direct identifiers
B. Identity federation
C. Cross-site scripting
D. Single sign-on
Answer: B (LEAVE A REPLY)

NEW QUESTION: 225
Which security concept, if implemented correctly, will protect the data on a system, even if a malicious actor gains access to the actual system?
A. Sandboxing
B. Encryption
C. Firewalls
D. Access control
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
In any environment, data encryption is incredibly important to prevent unauthorized exposure of data either internally or externally. If a system is compromised by an attack, having the data encrypted on the system will prevent its unauthorized exposure or export, even with the system itself being exposed.