ISC.CCSP.v2022-02-12.q575

Exam Code:	CCSP
Exam Name:	Certified Cloud Security Professional
Certification Provider:	ISC
Free Question Number:	575
Version:	v2022-02-12
# of views:	8165
# of Questions views:	5750
https://www.dumpsdb.com/dumps/ISC/CCSP/ISC.CCSP.v2022-02-12.q575	

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

NEW QUESTION: 2
What does dynamic application security testing (DAST) NOT entail?
A. Scanning
B. Probing
C. Discovery
D. Knowledge of the system
Answer: (SHOW ANSWER)

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

NEW QUESTION: 3
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: 4
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. Essential BCDR team members
C. Users
D. Regulators
Answer: A (LEAVE A REPLY)

NEW QUESTION: 5
Which protocol, as a part of TLS, handles negotiating and establishing a connection between two parties?
A. Record
B. Binding
C. Negotiation
D. Handshake
Answer: (SHOW ANSWER)
Explanation
The TLS handshake protocol is what negotiates and establishes the TLS connection between two parties and enables a secure communications channel to then handle data transmissions. The TLS record protocol is the actual secure communications method for transmitting data; it's responsible for the encryption and authentication of packets

throughout their transmission between the parties, and in some cases it also performs compression. Negotiation and binding are not protocols under TLS.

NEW QUESTION: 6
Which of the following threat types involves an application developer leaving references to internal information and configurations in code that is exposed to the client?
A. Sensitive data exposure
B. Security misconfiguration
C. Insecure direct object references
D. Unvalidated redirect and forwards
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
An insecure direct object reference occurs when a developer has in their code a reference to something on the application side, such as a database key, the directory structure of the application, configuration information about the hosting system, or any other information that pertains to the workings of the application that should not be exposed to users or the network. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, allowing spoofing for malware of phishing attacks.
Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data. Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner.

NEW QUESTION: 7
What type of data does data rights management (DRM) protect?
A. Consumer
B. PII
C. Financial
D. Healthcare
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
DRM applies to the protection of consumer media, such as music, publications, video, movies, and soon.

NEW QUESTION: 8
Which of the following would NOT be a reason to activate a BCDR strategy?
A. Staffing loss
B. Terrorism attack

C. Utility disruptions
D. Natural disaster
Answer: A (LEAVE A REPLY)
The loss of staffing would not be a reason to declare a BCDR situation because it does not impact production operations or equipment, and the same staff would be needed for a BCDR situation.

NEW QUESTION: 9
You have been tasked with creating an audit scope statement and are making your project outline.
Which of the following is NOT typically included in an audit scope statement?
A. Classification
B. Costs
C. Statement of purpose
D. Deliverables
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
Within a federated identity system, which entity accepts tokens from the identity provider?
A. Assertion manager
B. Servicing party
C. Proxy party
D. Relying party
Answer: D (LEAVE A REPLY)
The relying party is attached to the application or service that a user is trying to access, and it accepts authentication tokens from the user's own identity provider in order to facilitate authentication and access.
The other terms provided are all associated with federated systems, but none is the correct choice in this case.

NEW QUESTION: 11
Which one of the following threat types to applications and services involves the sending of requests that are invalid and manipulated through a user's client to execute commands on the application under the user's own credentials?
A. Injection
B. Missing function-level access control
C. Cross-site scripting
D. Cross-site request forgery
Answer: D (LEAVE A REPLY)
A cross-site request forgery (CSRF) attack forces a client that a user has used to authenticate to an application to send forged requests under the user's own credentials to

execute commands and requests that the application thinks are coming from a trusted client and user. Although this type of attack cannot be used to steal data directly because the attacker has no way of seeing the results of the commands, it does open other ways to compromise an application. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call.
Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries.

NEW QUESTION: 12
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)
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: 13
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)
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: 14
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
iSCSI does not natively support encryption, so another technology such as IPsec must be used to encrypt communications.

NEW QUESTION: 15
What is the concept of isolating an application from the underlying operating system for testing purposes?
A. Abstracting
B. Application virtualization
C. Hosting
D. Sandboxing
Answer: B (LEAVE A REPLY)
Explanation
Application virtualization is a software implementation that allows applications and programs to run in an isolated environment rather than directly interacting with the operating system. Sandboxing refers to segregating information or processes for security or testing purposes, but it's not directly related to isolation from the underlying operating system. Abstracting sounds similar to the correct term but is not pertinent to the question, and hosting is provided as an erroneous answer.

NEW QUESTION: 16
DLP solutions typically involve all of the following aspects except _____.
Response:
A. Data discovery
B. Enforcement
C. Monitoring
D. Tokenization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
Which component of ITIL involves the creation of an RFC ticket and obtaining official approvals for it?
A. Problem management
B. Release management
C. Deployment management
D. Change management
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The change management process involves the creation of the official Request for Change (RFC) ticket, which is used to document the change, obtain the required approvals from management and stakeholders, and track the change to completion. Release management is a subcomponent of change management, where the actual code or configuration change is put into place. Deployment management is similar to release management, but it's where changes are actually implemented on systems. Problem management is focused on the identification and mitigation of known problems and deficiencies before they are able to occur.

NEW QUESTION: 18
Which of the following report is most aligned with financial control audits?
A. SSAE 16
B. SOC 2
C. SOC 1
D. SOC 3
Answer: C (LEAVE A REPLY)
The SOC 1 report focuses primarily on controls associated with financial services. While IT controls are certainly part of most accounting systems today, the focus is on the controls around those financial systems.

NEW QUESTION: 19
When a system needs to be exposed to the public Internet, what type of secure system would be used to perform only the desired operations?

A. Firewall
B. Proxy
C. Honeypot
D. Bastion
Answer: D (LEAVE A REPLY)
A bastion is a system that is exposed to the public Internet to perform a specific function, but it is highly restricted and secured to just that function. Any nonessential services and access are removed from the bastion so that security countermeasures and monitoring can be focused just on the bastion's specific duties. A honeypot is a system designed to look like a production system to entice attackers, but it does not contain any real data. It is used for learning about types of attacks and enabling countermeasures for them. A firewall is used within a network to limit access between IP addresses and ports. A proxy server provides additional security to and rulesets for network traffic that is allowed to pass through it to a service destination.

NEW QUESTION: 20
Which of the following threat types involves the sending of invalid and manipulated requests through a user's client to execute commands on the application under their own credentials?
A. Injection
B. Cross-site request forgery
C. Missing function-level access control
D. Cross-site scripting
Answer: B (LEAVE A REPLY)
A cross-site request forgery (CSRF) attack forces a client that a user has used to authenticate to an application to send forged requests under the user's own credentials to execute commands and requests that the application thinks are coming from a trusted client and user. Although this type of attack cannot be used to steal data directly because the attacker has no way to see the results of the commands, it does open other ways to compromise an application. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes.

NEW QUESTION: 21
Which technique involves replacing values within a specific data field to protect sensitive data?
A. Anonymization

B. Masking
C. Tokenization
D. Obfuscation
Answer: B (LEAVE A REPLY)
Masking involves replacing specific data within a data set with new values. For example, with credit card fields, as most who have ever purchased anything online can attest, nearly the entire credit card number is masked with a character such as an asterisk, with the last four digits left visible for identification and confirmation.

NEW QUESTION: 22
When using an Infrastructure as a Service (IaaS) solution, what is the capability provided to the customer?
Response:
A. To provision processing, storage, networks, and other fundamental computing resources when the consumer is not able to deploy and run arbitrary software, which can include operating systems and applications.
B. To provision processing, storage, networks, and other fundamental computing resources when the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.
C. To provision processing, storage, networks, and other fundamental computing resources when the provider is able to deploy and run arbitrary software, which can include operating systems and applications.
D. To provision processing, storage, networks, and other fundamental computing resources when the auditor is able to deploy and run arbitrary software, which can include operating systems and applications.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
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)
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: 24
What are the phases of a software development lifecycle process model?
A. Planning and requirements analysis, design, define, develop, testing, and maintenance
B. Planning and requirements analysis, define, design, develop, testing, and maintenance
C. Define, planning and requirements analysis, design, develop, testing, and maintenance
D. Planning and requirements analysis, define, design, testing, develop, and maintenance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
What is the concept of segregating information or processes, within the same system or application, for security reasons?
A. fencing
B. Sandboxing
C. Cellblocking
D. Pooling
Answer: B (LEAVE A REPLY)
Sandboxing involves segregating and isolating information or processes from others within the same system or application, typically for security concerns. This is generally used for data isolation (for example, keeping different communities and populations of users isolated from other similar data).

NEW QUESTION: 26
Which of the following features is a main benefit of PaaS over IaaS?
A. Location independence
B. High-availability
C. Physical security requirements
D. Auto-scaling
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
With PaaS providing a fully configured and managed framework, auto-scaling can be implemented to programmatically adjust resources based on the current demands of the environment.

NEW QUESTION: 27
Which of the following threat types can occur when baselines are not appropriately applied or when unauthorized changes are made?
A. Security misconfiguration
B. Insecure direct object references
C. Unvalidated redirects and forwards

D. Sensitive data exposure

Answer: (SHOW ANSWER)

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: 28

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

A. IPS

B. WAF

C. DLP

D. IDS

Answer: C (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 29

What is the correct order of the phases of the data life cycle?

A. Create, Use, Store, Share, Archive, Destroy

B. Create, Archive, Store, Share, Use, Destroy

C. Create, Store, Use, Archive, Share, Destroy

D. Create, Store, Use, Share, Archive, Destroy

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The other options are the names of the phases, but out of proper order.

NEW QUESTION: 30

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

A. DoS/DDoS

B. Information bleed
C. Risk of loss/disclosure due to legal seizures
D. Escalation of privilege
Answer: A (LEAVE A REPLY)
DoS/DDoS threats and risks are not unique to the public cloud model.

NEW QUESTION: 31
Which of the following is NOT one of the main intended goals of a DLP solution?
A. Showing due diligence
B. Preventing malicious insiders
C. Regulatory compliance
D. Managing and minimizing risk
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Data loss prevention (DLP) extends the capabilities for data protection beyond the standard and traditional security controls that are offered by operating systems, application containers, and network devices. DLP is not specifically implemented to counter malicious insiders, and would not be particularly effective in doing so, because a malicious insider with legitimate access would have other ways to obtain data. DLP is a set of practices and controls to manage and minimize risk, comply with regulatory requirements, and show due diligence with the protection of data.

NEW QUESTION: 32
At which stage of the BCDR plan creation phase should security be included in discussions?
A. Define scope
B. Analyze
C. Assess risk
D. Gather requirements
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 33
Which of the following is the sole responsibility of the cloud provider, regardless of which cloud model is used?
A. Platform
B. Data
C. Physical environment
D. Infrastructure
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Regardless of which cloud-hosting model is used, the cloud provider always has sole responsibility for the physical environment.

NEW QUESTION: 34
Within a SaaS environment, what is the responsibility on the part of the cloud customer in regard to procuring the software used?
A. Maintenance
B. Licensing
C. Development
D. Purchasing
Answer: (SHOW ANSWER)
Explanation
Within a SaaS implementation, the cloud customer licenses the use of the software from the cloud provider because SaaS delivers a fully functional application to the customer. With SaaS, the cloud provider is responsible for the entire software application and any necessary infrastructure to develop, run, and maintain it. The purchasing, development, and maintenance are fully the responsibility of the cloud provider.

NEW QUESTION: 35
At which phase of the SDLC process should security begin participating?
A. Requirements gathering
B. Requirements analysis
C. Design
D. Testing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 36

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: (SHOW ANSWER)
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: 37
Which of the following is the best example of a key component of regulated PII?
A. Audit rights of subcontractors
B. Items that should be implemented
C. PCI DSS
D. Mandatory breach reporting
Answer: D (LEAVE A REPLY)
Mandatory breach reporting is the best example of regulated PII components. The rest are generally considered components of contractual PII.

NEW QUESTION: 38
Which of the following standards primarily pertains to cabling designs and setups in a data center?
A. IDCA
B. BICSI
C. NFPA
D. Uptime Institute
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The standards put out by Building Industry Consulting Service International (BICSI) primarily cover complex cabling designs and setups for data centers, but also include specifications on power, energy efficiency, and hot/cold aisle setups.

NEW QUESTION: 39
The cloud customer will have the most control of their data and systems, and the cloud provider will have the least amount of responsibility, in which cloud computing arrangement?
A. IaaS
B. SaaS

C. Community cloud
D. PaaS
Answer: A (LEAVE A REPLY)
Explanation
IaaS entails the cloud customer installing and maintaining the OS, programs, and data; PaaS has the customer installing programs and data; in SaaS, the customer only uploads data. In a community cloud, data and device owners are distributed.

NEW QUESTION: 40
In general, a cloud BCDR solution will be _____ than a physical solution.
Response:
A. More difficult to engineer
B. Larger
C. Slower
D. Less expensive
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
Which ISO/IEC standards set documents the cloud definitions for staffing and official roles?
Response:
A. ISO/IEC 27040
B. ISO/IEC 17788
C. ISO/IEC 27001
D. ISO/IEC 17789
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
If bit-splitting is used to store data sets across multiple jurisdictions, how may this enhance security?
Response:
A. By restricting privilege user access
B. By making seizure of data by law enforcement more difficult
C. By ensuring that users can only accidentally disclose data to one geographic area
D. By hiding it from attackers in a specific jurisdiction
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?
Response:

A. Cross-site request forgery
B. Unvalidated redirects and forwards
C. Insecure direct object references
D. Cross-site scripting
Answer: (SHOW ANSWER)

NEW QUESTION: 44
What does dynamic application security testing (DAST) NOT entail?
A. Scanning
B. Probing
C. Discovery
D. Knowledge of the system
Answer: D (LEAVE A REPLY)
Explanation
Dynamic application security testing (DAST) is considered "black box" testing and begins with no inside knowledge of the application or its configurations. Everything about the application must be discovered during the testing.

NEW QUESTION: 45
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)
Explanation
Portability is the ability for a cloud customer to easily move their systems, services, and applications among different cloud providers. By avoiding reliance on proprietary APIs and other vendor-specific cloud features, an organization can maintain flexibility to move among the various cloud providers with greater ease.
Reversibility refers to the ability for a cloud customer to quickly and easy remove all their services and data from a cloud provider. Interoperability is the ability to reuse services and components for other applications and uses. Scalability refers to the ability of a cloud environment to add or remove resources to meet current demands.

NEW QUESTION: 46
Which of the following pertains to a macro level approach to data center design rather than the traditional tiered approach to data centers?
A. IDCA

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

NEW QUESTION: 47
When a system needs to be exposed to the public Internet, what type of secure system would be used to perform only the desired operations?
A. Firewall
B. Proxy
C. Honeypot
D. Bastion
Answer: D (LEAVE A REPLY)
Explanation
A bastion is a system that is exposed to the public Internet to perform a specific function, but it is highly restricted and secured to just that function. Any nonessential services and access are removed from the bastion so that security countermeasures and monitoring can be focused just on the bastion's specific duties. A honeypot is a system designed to look like a production system to entice attackers, but it does not contain any real data. It is used for learning about types of attacks and enabling countermeasures for them. A firewall is used within a network to limit access between IP addresses and ports. A proxy server provides additional security to and rulesets for network traffic that is allowed to pass through it to a service destination.

NEW QUESTION: 48
Which of the following methods is often used to obscure data from production systems for use in test or development environments?
A. Tokenization
B. Encryption
C. Classification
D. Masking
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which of the following roles involves the connection and integration of existing systems and services to a cloud environment?
A. Cloud service business manager
B. Cloud service user
C. Cloud service administrator
D. Cloud service integrator
Answer: (SHOW ANSWER)
Explanation
The cloud service integrator is the official role that involves connecting and integrating existing systems and services with a cloud environment. This may involve moving services into a cloud environment, or connecting to external cloud services and capabilities from traditional data center-hosted services.

NEW QUESTION: 50
DLP solutions typically involve all of the following aspects except _____.
A. Monitoring
B. Tokenization
C. Enforcement
D. Data discovery
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
Maintenance mode requires all of these actions except:
A. Remove all active production instances
B. Ensure logging continues
C. Initiate enhanced security controls
D. Prevent new logins
Answer: (SHOW ANSWER)
While the other answers are all steps in moving from normal operations to maintenance mode, we do not necessarily initiate any enhanced security controls.

NEW QUESTION: 52
What are the four cloud deployment models?
A. Public, Internal, Hybrid, and Community
B. External, Private, Hybrid, and Community
C. Public, Private, Hybrid, and Community
D. Public, Private, Joint, and Community
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
Which of the following threat types can occur when encryption is not properly applied or insecure transport mechanisms are used?
A. Security misconfiguration
B. Insecure direct object references
C. Sensitive data exposure
D. Unvalidated redirects and forwards
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Sensitive data exposure occurs when information is not properly secured through encryption and secure transport mechanisms; it can quickly become an easy and broad method for attackers to compromise information. Web applications must enforce strong encryption and security controls on the application side, but secure methods of communications with browsers or other clients used to access the information are also required. Security misconfiguration occurs when applications and systems are not properly configured for security, often a result of misapplied or inadequate baselines. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, thus allowing spoofing for malware or phishing attacks.

NEW QUESTION: 54
The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program has
_____ tiers.
A. Four
B. Two
C. Three
D. Eight
Answer: (SHOW ANSWER)

NEW QUESTION: 55
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: 56
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The data owner is usually considered the cloud customer in a cloud configuration; the data in question is the customer's information, being processed in the cloud. The cloud provider is only leasing services and hardware to the customer. The cloud access security broker (CASB) only handles access control on behalf of the cloud customer, and is not in direct contact with the production data.

NEW QUESTION: 57
In the wake of many scandals with major corporations involving fraud and the deception of investors and regulators, which of the following laws was passed to govern accounting and financial records and disclosures?
A. GLBA
B. Safe Harbor
C. HIPAA
D. SOX
Answer: (SHOW ANSWER)
The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and accounting

errors.The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy.
The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions.
The Safe Harbor program was designed by the US government as a way for American companies to comply with European Union privacy laws.

NEW QUESTION: 58
Many activities within a cloud environment are performed via programmatic means, where complex and distributed operations are handled without the need to perform each step individually.
Which of the following concepts does this describe?
A. Orchestration
B. Provisioning
C. Automation
D. Allocation
Answer: A (LEAVE A REPLY)
Orchestration is the programmatic means of managing and coordinating activities within a cloud environment and allowing for a commensurate level of automation and self-service. Provisioning, allocation, and automation are all components of orchestration, but none refers to the overall concept.

NEW QUESTION: 59
Which of the following is the concept of segregating information or processes, within the same system or application, for security reasons?
A. Cell blocking
B. Sandboxing
C. Pooling
D. Fencing
Answer: B (LEAVE A REPLY)
Sandboxing involves the segregation and isolation of information or processes from other information or processes within the same system or application, typically for security concerns. Sandboxing is generally used for data isolation (for example, keeping different communities and populations of users isolated from others with similar data). In IT terminology, pooling typically means bringing together and consolidating resources or services, not segregating or separating them. Cell blocking and fencing are both erroneous terms.

NEW QUESTION: 60
Countermeasures for protecting cloud operations against internal threats include all of the following except:

A. Extensive and comprehensive training programs, including initial, recurring, and refresher sessions
B. Skills and knowledge testing
C. Hardened perimeter devices
D. Aggressive background checks
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Hardened perimeter devices are more useful at attenuating the risk of external attack.

NEW QUESTION: 61
Which of the following roles involves the provisioning and delivery of cloud services?
A. Cloud service deployment manager
B. Cloud service business manager
C. Cloud service manager
D. Cloud service operations manager
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The cloud service manager is responsible for the delivery of cloud services, the provisioning of cloud services, and the overall management of cloud services.

NEW QUESTION: 62
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: 63
The Restatement (Second) Conflict of Law refers to which of the following?
Response:
A. When judges restate the law in an opinion
B. How jurisdictional disputes are settled
C. The basis for deciding which laws are most appropriate in a situation where conflicting laws exist
D. Whether local or federal laws apply in a situation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 64
Which protocol allows a system to use block-level storage as if it was a SAN, but over TCP network traffic instead?
A. SATA
B. iSCSI
C. TLS
D. SCSI
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
iSCSI is a protocol that allows for the transmission and use of SCSI commands and features over a TCP- based network. iSCSI allows systems to use block-level storage that looks and behaves as a SAN would with physical servers, but to leverage the TCP network within a virtualized environment and cloud.

NEW QUESTION: 65
Which component of ITIL pertains to planning, coordinating, executing, and validating changes and rollouts to production environments?
A. Release management
B. Availability management
C. Problem management
D. Change management
Answer: (SHOW ANSWER)
Release management involves planning, coordinating, executing, and validating changes and rollouts to the production environment. Change management is a higher-level component than release management and also involves stakeholder and management approval, rather than specifically focusing the actual release itself. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION: 66
DNSSEC was designed to add a layer of security to the DNS protocol.
Which type of attack was the DNSSEC extension designed to mitigate?
A. Account hijacking
B. Snooping
C. Spoofing
D. Data exposure
Answer: C (LEAVE A REPLY)
Explanation
DNSSEC is an extension to the regular DNS protocol that utilizes digital signing of DNS query results, which can be verified to come from an authoritative source. This verification mitigates the ability for a rogue DNS server to be used to spoof query results and to direct users to malicious sites. DNSSEC provides for the verification of the integrity of DNS queries. It does not provide any protection from snooping or data exposure. Although it may help lessen account hijacking by preventing users from being directed to rogue sites, it cannot by itself eliminate the possibility.

NEW QUESTION: 67
What strategy involves replacing sensitive data with opaque values, usually with a means of mapping it back to the original value?
A. Masking
B. Anonymization
C. Tokenization
D. Obfuscation
Answer: C (LEAVE A REPLY)
Explanation
Tokenization is the practice of utilizing a random and opaque "token" value in data to replace what otherwise would be a sensitive or protected data object. The token value is usually generated by the application with a means to map it back to the actual real value, and then the token value is placed in the data set with the same formatting and requirements of the actual real value so that the application can continue to function without different modifications or code changes.

NEW QUESTION: 68
When data discovery is undertaken, three main approaches or strategies are commonly used to determine what the type of data, its format, and composition are for the purposes of classification.
Which of the following is NOT one of the three main approaches to data discovery?
A. Content analysis
B. Hashing

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

NEW QUESTION: 69
What process entails taking sensitive data and removing the indirect identifiers from each data object so that the identification of a single entity would not be possible?
A. Tokenization
B. Encryption
C. Anonymization
D. Masking
Answer: C (LEAVE A REPLY)
Anonymization is a type of masking, where indirect identifiers are removed from a data set to prevent the mapping back of data to an individual. Although masking refers to the overall approach of covering sensitive data, anonymization is the best answer here because it is more specific to exactly what is being asked. Tokenization involves the replacement of sensitive data with a key value that can be matched back to the real value. However, it is not focused on indirect identifiers or preventing the matching to an individual. Encryption refers to the overall process of protecting data via key pairs and protecting confidentiality.

NEW QUESTION: 70
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: 71
The cloud customer's trust in the cloud provider can be enhanced by all of the following except:
A. SLAs
B. Shared administration
C. Audits
D. real-time video surveillance
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Video surveillance will not provide meaningful information and will not enhance trust. All the others will do it.

NEW QUESTION: 72
The application normative framework is best described as which of the following?
A. A superset of the ONF
B. A stand-alone framework for storing security practices for the ONF
C. The complete ONF
D. A subnet of the ONF
Answer: D (LEAVE A REPLY)
Remember, there is a one-to-many ratio of ONF to ANF; each organization has one ONF and many ANFs (one for each application in the organization). Therefore, the ANF is a subset of the ONF.

NEW QUESTION: 73
Which security concept is focused on the trustworthiness of data?
A. Integrity
B. Availability
C. Nonrepudiation
D. Confidentiality
Answer: A (LEAVE A REPLY)
Integrity is focused on the trustworthiness of data as well as the prevention of unauthorized modification or tampering of it. A prime consideration for maintaining integrity is an emphasis on the change management and configuration management aspects of operations, so that all modifications are predictable, tracked, logged, and verified, whether they are performed by actual human users or systems processes and scripts.

NEW QUESTION: 74
What must SOAP rely on for security?
A. Encryption

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

NEW QUESTION: 75
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.

NEW QUESTION: 76
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)
Explanation
When a security professional is considering cloud solutions for BCDR, a top concern is the jurisdiction where the cloud systems are hosted. If the jurisdiction is different from where the production systems are hosted, they may be subjected to different regulations and controls, which would make a seamless BCDR solution far more difficult.

NEW QUESTION: 77
In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?
A. HIPAA
B. The contract
C. Statutes
D. Security control matrix
Answer: B (LEAVE A REPLY)
Explanation
The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable. The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

NEW QUESTION: 78
Data labels could include all the following, except:
A. Distribution limitations
B. Multifactor authentication
C. Confidentiality level
D. Access restrictions
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
All the others might be included in data labels, but multifactor authentication is a procedure used for access control, not a label.

NEW QUESTION: 79
A firewall can use all of the following techniques for controlling traffic except:
A. Randomization
B. Rule sets
C. Content filtering
D. Behavior analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80

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

A. Segregated from host systems

B. Network access

C. Scalability

D. External to system patching

Answer: (SHOW ANSWER)

Explanation

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

Network access is not a consideration because both a host-based IDS and a network-based IDS would have access to network resources.

NEW QUESTION: 81

Which of the following represents a minimum guaranteed resource within a cloud environment for the cloud customer?

A. Reservation

B. Share

C. Limit

D. Provision

Answer: (SHOW ANSWER)

Explanation

A reservation is a minimum resource that is guaranteed to a customer within a cloud environment. Within a cloud, a reservation can pertain to the two main aspects of computing: memory and processor. With a reservation in place, the cloud provider guarantees that a cloud customer will always have at minimum the necessary resources available to power on and operate any of their services.

NEW QUESTION: 82

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

A. IDCA

B. BICSI

C. NFPA

D. Uptime Institute

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

NEW QUESTION: 83
What concept does the D represent within the STRIDE threat model?
A. Denial of service
B. Distributed
C. Data breach
D. Data loss
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Any application can be a possible target of denial of service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for unauthenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks. None of the other options provided is the correct term.

NEW QUESTION: 84
Which of the following threat types can occur when baselines are not appropriately applied or unauthorized changes are made?
A. Insecure direct object references
B. Unvalidated redirects and forwards
C. Security misconfiguration
D. Sensitive data exposure
Answer: (SHOW ANSWER)
Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner. This can be caused from 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.

NEW QUESTION: 85
Which of the following BCDR testing methodologies is least intrusive?
Response:
A. Tabletop
B. Simulation
C. Walk-through
D. Full test
Answer: A (LEAVE A REPLY)

NEW QUESTION: 86
Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?
A. Regulation
B. Multitenancy
C. Virtualization
D. Resource pooling
Answer: B (LEAVE A REPLY)
With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers. Especially within a public cloud model, it is not possible or practical for a cloud provider to alter its services for specific customer demands. Resource pooling and virtualization within a cloud environment would be the same for all customers, and would not impact certifications that a cloud provider might be willing to pursue. Regulations would form the basis for certification problems and would be a reason for a cloud provider to pursue specific certifications to meet customer requirements.

NEW QUESTION: 87
DNSSEC was designed to add a layer of security to the DNS protocol.
Which type of attack was the DNSSEC extension designed to mitigate?
A. Account hijacking
B. Snooping
C. Spoofing
D. Data exposure
Answer: C (LEAVE A REPLY)
DNSSEC is an extension to the regular DNS protocol that utilizes digital signing of DNS query results, which can be verified to come from an authoritative source. This verification mitigates the ability for a rogue DNS server to be used to spoof query results and to direct users to malicious sites. DNSSEC provides for the verification of the integrity of DNS queries. It does not provide any protection from snooping or data exposure. Although it may help lessen account hijacking by preventing users from being directed to rogue sites, it cannot by itself eliminate the possibility.

NEW QUESTION: 88
Which of the following represents a prioritization of applications or cloud customers for the allocation of additional requested resources when there is a limitation on available resources?
A. Provision
B. Limit

C. Reservation
D. Share
Answer: (SHOW ANSWER)
Explanation
The concept of shares within a cloud environment is used to mitigate and control the request for resource allocations from customers that the environment may not have the current capability to allow. Shares work by prioritizing hosts within a cloud environment through a weighting system that is defined by the cloud provider.
When periods of high utilization and allocation are reached, the system automatically uses scoring of each host based on its share value to determine which hosts get access to the limited resources still available. The higher the value a particular host has, the more resources it will be allowed to utilize.

NEW QUESTION: 89
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: 90
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: (SHOW ANSWER)
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: 91
Which of the following can be useful for protecting cloud customers from a denial-of-service (DoS) attack against another customer hosted in the same cloud?
A. Reservations
B. Measured service
C. Limits
D. Shares
Answer: A (LEAVE A REPLY)
Reservations ensure that a minimum level of resources will always be available to a cloud customer for them to start and operate their services. In the event of a DoS attack against one customer, they can guarantee that the other customers will still be able to operate.

NEW QUESTION: 92
What is the intellectual property protection for a confidential recipe for muffins?
A. Patent
B. Trademark
C. Trade secret

D. Copyright
Answer: C (LEAVE A REPLY)
Confidential recipes unique to the organization are trade secrets. The other answers listed are answers to other questions.

NEW QUESTION: 93
With IaaS, what is responsible for handling the security and control over the volume storage space?
A. Management plane
B. Operating system
C. Application
D. Hypervisor
Answer: B (LEAVE A REPLY)
Explanation
Volume storage is allocated via a LUN to a system and then treated the same as any traditional storage. The operating system is responsible for formatting and securing volume storage as well as controlling all access to it. Applications, although they may use volume storage and have permissions to write to it, are not responsible for its formatting and security. Both a hypervisor and the management plane are outside of an individual system and are not responsible for managing the files and storage within that system.

NEW QUESTION: 94
Although the REST API supports a wide variety of data formats for communications and exchange, which data formats are the most commonly used?
A. SAML and HTML
B. XML and SAML
C. XML and JSON
D. JSON and SAML
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API and are typically implemented with caching for increased scalability and performance. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data.
HTML is used for authoring web pages for consumption by web browsers

NEW QUESTION: 95

Which of the following is a management role, versus a technical role, as it pertains to data management and oversight?

A. Data owner

B. Data processor

C. Database administrator

D. Data custodian

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Data owner is a management role that's responsible for all aspects of how data is used and protected. The database administrator, data custodian, and data processor are all technical roles that involve the actual use and consumption of data, or the implementation of security controls and policies with the data.

NEW QUESTION: 96

Each of the following is an element of the Identification phase of the identity and access management (IAM) process except _____.

A. Inversion

B. Deprovisioning

C. Management

D. Provisioning

Answer: A (LEAVE A REPLY)

NEW QUESTION: 97

Which cloud service category most commonly uses client-side key management systems?

A. Software as a Service

B. Infrastructure as a Service

C. Platform as a Service

D. Desktop as a Service

Answer: (SHOW ANSWER)

SaaS most commonly uses client-side key management. With this type of implementation, the software for doing key management is supplied by the cloud provider, but is hosted and run by the cloud customer.

This allows for full integration with the SaaS implementation, but also provides full control to the cloud customer. Although the cloud provider may offer software for performing key management to the cloud customers, with the Infrastructure, Platform, and Desktop as a Service categories, the customers would largely be responsible for their own options and implementations and would not be bound by the offerings from the cloud provider.

NEW QUESTION: 98

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: 99
Which of the following service categories entails the least amount of support needed on the part of the cloud customer?
A. SaaS
B. IaaS
C. DaaS
D. PaaS
Answer: (SHOW ANSWER)
With SaaS providing a fully functioning application that is managed and maintained by the cloud provider, cloud customers incur the least amount of support responsibilities themselves of any service category.

NEW QUESTION: 100
Modern web service systems are designed for high availability and resiliency. Which concept pertains to the ability to detect problems within a system, environment, or application and programmatically invoke redundant systems or processes for mitigation?
A. Elasticity
B. Redundancy
C. Fault tolerance
D. Automation
Answer: (SHOW ANSWER)
Fault tolerance allows a system to continue functioning, even with degraded performance, if portions of it fail or degrade, without the entire system or service being taken down. It can detect problems within a service and invoke compensating systems or functions to keep functionality going. Although redundancy is similar to fault tolerance, it is more focused on having additional copies of systems available, either active or passive, that can take up services if one system goes down. Elasticity pertains to the ability of a system to resize to meet demands, but it is not focused on system failures. Automation, and its role in

maintaining large systems with minimal intervention, is not directly related to fault tolerance.

NEW QUESTION: 101
BCDR strategies do not typically involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the amount of services that need to be recovered to meet BCDR objectives?
A. RSL
B. RTO
C. RPO
D. SRE
Answer: (SHOW ANSWER)
The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the determined level of operations necessary during a BCDR situation. The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. SRE is provided as an erroneous response.

NEW QUESTION: 102
One of the main components of system audits is the ability to track changes over time and to match these changes with continued compliance and internal processes.
Which aspect of cloud computing makes this particular component more challenging than in a traditional data center?
A. Portability
B. Virtualization
C. Elasticity
D. Resource pooling
Answer: B (LEAVE A REPLY)
Cloud services make exclusive use of virtualization, and systems change over time, including the addition, subtraction, and reimaging of virtual machines. It is extremely unlikely that the exact same virtual machines and images used in a previous audit would still be in use or even available for a later audit, making the tracking of changes over time extremely difficult, or even impossible. Elasticity refers to the ability to add and remove resources from a system or service to meet current demand, and although it plays a factor in making the tracking of virtual machines very difficult over time, it is not the best answer in this case. Resource pooling pertains to a cloud environment sharing a large amount of resources between different customers and services. Portability refers to the ability to move systems or services easily between different cloud providers.

NEW QUESTION: 103
Which type of cloud model typically presents the most challenges to a cloud customer during the
"destroy" phase of the cloud data lifecycle?
A. IaaS
B. DaaS
C. SaaS
D. PaaS
Answer: C (LEAVE A REPLY)
With many SaaS implementations, data is not isolated to a particular customer but rather is part of the overall application. When it comes to data destruction, a particular challenge is ensuring that all of a customer's data is completely destroyed while not impacting the data of other customers.

NEW QUESTION: 104
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: (SHOW ANSWER)
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: 105
Which of the following is NOT part of a retention policy?
A. Format
B. Costs
C. Accessibility
D. Duration
Answer: B (LEAVE A REPLY)
The data retention policy covers the duration, format, technologies, protection, and accessibility of archives, but does not address the specific costs of its implementation and maintenance.

NEW QUESTION: 106
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)
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: 107
Which crucial aspect of cloud computing can be most threatened by insecure APIs?
A. Automation
B. Resource pooling
C. Elasticity
D. Redundancy
Answer: A (LEAVE A REPLY)
Explanation
Cloud environments depend heavily on API calls for management and automation. Any vulnerability with the APIs can cause significant risk and exposure to all tenants of the cloud environment. Resource pooling and elasticity could both be impacted by insecure APIs, as both require automation and orchestration to operate properly, but automation is the better answer here. Redundancy would not be directly impacted by insecure APIs.

NEW QUESTION: 108
Which of the following is NOT considered a type of data loss?
A. Data corruption
B. Stolen by hackers
C. Accidental deletion
D. Lost or destroyed encryption keys
Answer: (SHOW ANSWER)

The exposure of data by hackers is considered a data breach. Data loss focuses on the data availability rather than security. Data loss occurs when data becomes lost, unavailable, or destroyed, when it should not have been.

NEW QUESTION: 109
What aspect of a Type 2 hypervisor involves additional security concerns that are not relevant with a Type 1 hypervisor?
Response:
A. Reliance on a host operating system
B. Proprietary software
C. Auditing
D. Programming languages
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which of the following threat types involves leveraging a user's browser to send untrusted data to be executed with legitimate access via the user's valid credentials?
A. Injection
B. Missing function-level access control
C. Cross-site scripting
D. Cross-site request forgery
Answer: D (LEAVE A REPLY)
Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or perhaps the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with their own access and permissions, allowing the attacker to redirect the user's web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access.
Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries.
Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.

NEW QUESTION: 111
When a system needs to be exposed to the public Internet, what type of secure system would be used to perform only the desired operations?
A. Firewall
B. Proxy

C. Honeypot
D. Bastion
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A bastion is a system that is exposed to the public Internet to perform a specific function, but it is highly restricted and secured to just that function. Any nonessential services and access are removed from the bastion so that security countermeasures and monitoring can be focused just on the bastion's specific duties. A honeypot is a system designed to look like a production system to entice attackers, but it does not contain any real data. It is used for learning about types of attacks and enabling countermeasures for them. A firewall is used within a network to limit access between IP addresses and ports. A proxy server provides additional security to and rulesets for network traffic that is allowed to pass through it to a service destination.

NEW QUESTION: 112
Although performing BCDR tests at regular intervals is a best practice to ensure processes and documentation are still relevant and efficient, which of the following represents a reason to conduct a BCDR review outside of the regular interval?
Response:
A. Regulatory changes
B. Management changes
C. Staff changes
D. Application changes
Answer: D (LEAVE A REPLY)

NEW QUESTION: 113
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: (SHOW ANSWER)
Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe. The rest are not.

NEW QUESTION: 114
The president of your company has tasked you with implementing cloud services as the most efficient way of obtaining a robust disaster recovery configuration for your production services.
Which of the cloud deployment models would you MOST likely be exploring?

A. Hybrid
B. Private
C. Community
D. Public
Answer: (SHOW ANSWER)
Explanation
A hybrid cloud model spans two more different hosting configurations or cloud providers. This would enable an organization to continue using its current hosting configuration, while adding additional cloud services to enable disaster recovery capabilities. The other cloud deployment models--public, private, and community--would not be applicable for seeking a disaster recovery configuration where cloud services are to be leveraged for that purpose rather than production service hosting.

NEW QUESTION: 115
Which document will enforce uptime and availability requirements between the cloud customer and cloud provider?
Response:
A. Service level agreement
B. Regulation
C. Contract
D. Operational level agreement
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
Which network protocol is essential for allowing automation and orchestration within a cloud environment?
Response:
A. DNSSEC
B. DHCP
C. VLANs
D. IPsec
Answer: B (LEAVE A REPLY)

NEW QUESTION: 117
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: 118
Countermeasures for protecting cloud operations against internal threats include all of the following except:
A. Mandatory vacation
B. Least privilege
C. Separation of duties
D. Conflict of interest
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Conflict of interest is a threat, not a control.

NEW QUESTION: 119
Which aspect of cloud computing will be most negatively impacted by vendor lock-in?
A. Elasticity
B. Reversibility
C. Interoperability
D. Portability
Answer: (SHOW ANSWER)
A cloud customer utilizing proprietary APIs or services from one cloud provider that are unlikely to be available from another cloud provider will most negatively impact portability.

NEW QUESTION: 120
DLP solutions can aid in deterring loss due to which of the following?
A. Inadvertent disclosure
B. Natural disaster
C. Randomization
D. Device failure
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
DLP solutions may protect against inadvertent disclosure. Randomization is a technique for obscuring data, not a risk to data. DLP tools will not protect against risks from natural disasters, or against impacts due to device failure.

NEW QUESTION: 121
Deviations from the baseline should be investigated and _____.

A. Revealed
B. Documented
C. Encouraged
D. Enforced
Answer: B (LEAVE A REPLY)
All deviations from the baseline should be documented, including details of the investigation and outcome. We do not enforce or encourage deviations. Presumably, we would already be aware of the deviation, so
"revealing" is not a reasonable answer.

NEW QUESTION: 122
Which data formats are most commonly used with the REST API?
A. JSON and SAML
B. XML and SAML
C. XML and JSON
D. SAML and HTML
Answer: C (LEAVE A REPLY)
Explanation
JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API, and are typically implemented with caching for increased scalability and performance.

NEW QUESTION: 123
SOC Type 1 reports are considered "restricted use," in that they are intended only for limited audiences and purposes.
Which of the following is NOT a population that would be appropriate for a SOC Type 1 report?
A. Current clients
B. Auditors
C. Potential clients
D. The service organization
Answer: C (LEAVE A REPLY)

Explanation/Reference:
Explanation:
Potential clients are not served by SOC Type 1 audits. A Type 2 or Type 3 report would be appropriate for potential clients. SOC Type 1 reports are intended for restricted use, where only the service organization itself, current clients, or auditors would have access to them.

NEW QUESTION: 124
To address shared monitoring and testing responsibilities in a cloud configuration, the provider might offer all these to the cloud customer except:
A. Access to audit logs and performance data
B. DLP solution results
C. Security control administration
D. SIM, SEIM. and SEM logs
Answer: C (LEAVE A REPLY)
While the provider might share any of the other options listed, the provider will not share administration of security controls with the customer. Security controls are the sole province of the provider.

NEW QUESTION: 125
Which of the following is a method for apportioning resources that involves setting guaranteed minimums for all tenants/customers within the environment?
Response:
A. Cancellations
B. Reservations
C. Limits
D. Shares
Answer: (SHOW ANSWER)

NEW QUESTION: 126
What are the phases of a software development lifecycle process model?
Response:
A. Planning and requirements analysis, design, define, develop, testing, and maintenance
B. Define, planning and requirements analysis, design, develop, testing, and maintenance
C. Planning and requirements analysis, define, design, develop, testing, and maintenance
D. Planning and requirements analysis, define, design, testing, develop, and maintenance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 127
With a cloud service category where the cloud customer is responsible for deploying all services, systems, and components needed for their applications, which of the following storage types are MOST likely to be available to them?

A. Structured and hierarchical
B. Volume and object
C. Volume and database
D. Structured and unstructured
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The question is describing the Infrastructure as a Service (IaaS) cloud offering, and as such, the volume and object storage types will be available to the customer. Structured and unstructured are storage types associated with PaaS, and although the other answers present similar-sounding storage types, they are a mix of real and fake names.

NEW QUESTION: 128
Which of the following could be used as a second component of multifactor authentication if a user has an RSA token?
A. Access card
B. USB thumb drive
C. Retina scan
D. RFID
Answer: C (LEAVE A REPLY)
Explanation
A retina scan could be used in conjunction with an RSA token because it is a biometric factor, and thus a different type of factor. An access card, RFID, and USB thumb drive are all items in possession of a user, the same as an RSA token, and as such would not be appropriate.

NEW QUESTION: 129
The European Union passed the first major regulation declaring data privacy to be a human right.
In what year did it go into effect?
A. 2010
B. 2000
C. 1995
D. 1990
Answer: (SHOW ANSWER)
Adopted in 1995, Directive 95/46 EC establishes strong data protection and policy requirements, including the declaring of data privacy to be a human right. It establishes that an individual has the right to be notified when their personal data is being access or processed, that it only will ever be accessed for legitimate purposes, and that data will only be accessed to the exact extent it needs to be for the particular process or request.

NEW QUESTION: 130
Which of the following is NOT considered a type of data loss?
A. Data corruption
B. Stolen by hackers
C. Accidental deletion
D. Lost or destroyed encryption keys
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The exposure of data by hackers is considered a data breach. Data loss focuses on the data availability rather than security. Data loss occurs when data becomes lost, unavailable, or destroyed, when it should not have been.

NEW QUESTION: 131
Which approach is typically the most efficient method to use for data discovery?
A. Metadata
B. Content analysis
C. Labels
D. ACLs
Answer: (SHOW ANSWER)
Explanation
Metadata is data about data. It contains information about the type of data, how it is stored and organized, or information about its creation and use.

NEW QUESTION: 132
In application-level encryption, where does the encryption engine reside?
Response:
A. Within the database accessed by the application
B. In the application accessing the database
C. In the volume where the database resides
D. In the OS on which the application is run
Answer: B (LEAVE A REPLY)

NEW QUESTION: 133
Which type of testing uses the same strategies and toolsets that hackers would use?
A. Penetration
B. Dynamic
C. Static
D. Malicious
Answer: A (LEAVE A REPLY)
Explanation/Reference:

Explanation:
Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discovery potential vulnerabilities.

NEW QUESTION: 134
You are developing a new process for data discovery for your organization and are charged with ensuring that all applicable data is included. Which of the following is NOT one of the three methods of data discovery?
Response:
A. Labels
B. Metadata
C. Classification
D. Content analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 135
Upon completing a risk analysis, a company has four different approaches to addressing risk.
Which approach it takes will be based on costs, available options, and adherence to any regulatory requirements from independent audits.
Which of the following groupings correctly represents the four possible approaches?
A. Accept, avoid, transfer, mitigate
B. Accept, deny, transfer, mitigate
C. Accept, deny, mitigate, revise
D. Accept, dismiss, transfer, mitigate
Answer: A (LEAVE A REPLY)
The four possible approaches to risk are as follows: accept (do not patch and continue with the risk), avoid (implement solutions to prevent the risk from occurring), transfer (take out insurance), and mitigate (change configurations or patch to resolve the risk). Each of these answers contains at least one incorrect approach name.

NEW QUESTION: 136
Apart from using encryption at the file system level, what technology is the most widely used to protect data stored in an object storage system?
A. TLS
B. HTTPS
C. VPN
D. IRM
Answer: D (LEAVE A REPLY)
Information rights management (IRM) technologies allow security controls and policies to be enforced on a data object regardless of where it resides. They also allow for extended

controls such as expirations and copying restrictions, which are not available through traditional control mechanisms. 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 and likely will be used in conjunction with other object data protection strategies.

NEW QUESTION: 137
Which of the following best describes the Organizational Normative Framework (ONF)?
A. A set of application security, and best practices, catalogued and leveraged by the organization
B. A container for components of an application's security, best practices catalogued and leveraged by the organization
C. A framework of containers for some of the components of application security, best practices, catalogued and leveraged by the organization
D. A framework of containers for all components of application security, best practices, catalogued and leveraged by the organization.
Answer: (SHOW ANSWER)
Explanation
Option B is incorrect, because it refers to a specific applications security elements, meaning it is about an ANF, not the ONF. C is true, but not as complete as D, making D the better choice. C suggests that the framework contains only "some" of the components, which is why B (which describes "all" components) is better

NEW QUESTION: 138
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: 139
Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.
Which of the following is NOT a regulatory system from the United States federal government?
A. HIPAA
B. SOX
C. FISMA
D. PCI DSS
Answer: D (LEAVE A REPLY)
The Payment Card Industry Data Security Standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry-regulatory standard, not a governmental one.
The Sarbanes-Oxley Act (SOX) was passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders.
The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

NEW QUESTION: 140
Within a federated identity system, which entity accepts tokens from the identity provider?
A. Assertion manager
B. Servicing party
C. Proxy party
D. Relying party
Answer: D (LEAVE A REPLY)
The relying party is attached to the application or service that a user is trying to access, and it accepts authentication tokens from the user's own identity provider in order to facilitate authentication and access. The other terms provided are all associated with federated systems, but none is the correct choice in this case.

NEW QUESTION: 141
Which of the following actions will NOT make data part of the "create" phase of the cloud data lifecycle?
A. Modifying metadata
B. Importing data
C. Modifying data
D. Constructing new data
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Although the 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 modified into a new form or value. Modifying the metadata does not change the actual data.

NEW QUESTION: 142
Which of the following roles involves the connection and integration of existing systems and services to a cloud environment?
A. Cloud service business manager
B. Cloud service user
C. Cloud service administrator
D. Cloud service integrator
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The cloud service integrator is the official role that involves connecting and integrating existing systems and services with a cloud environment. This may involve moving services into a cloud environment, or connecting to external cloud services and capabilities from traditional data center-hosted services.

NEW QUESTION: 143
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: 144
A loosely coupled storage cluster will have performance and capacity limitations based on the _____.
Response:
A. Amount of usage demanded
B. Total number of nodes in the cluster
C. Physical backplane connecting it
D. The performance and capacity in each node
Answer: (SHOW ANSWER)

NEW QUESTION: 145
Within a SaaS environment, what is the responsibility on the part of the cloud customer in regard to procuring the software used?
A. Maintenance
B. Licensing
C. Development
D. Purchasing
Answer: B (LEAVE A REPLY)
Within a SaaS implementation, the cloud customer licenses the use of the software from the cloud provider because SaaS delivers a fully functional application to the customer. With SaaS, the cloud provider is responsible for the entire software application and any necessary infrastructure to develop, run, and maintain it.
The purchasing, development, and maintenance are fully the responsibility of the cloud provider.

NEW QUESTION: 146
What is used for local, physical access to hardware within a data center?
A. SSH
B. KVM
C. VPN
D. RDP

Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Local, physical access in a data center is done via KVM (keyboard, video, mouse) switches.

NEW QUESTION: 147
Managed cloud services exist because the service is less expensive for each customer than creating the same services for themselves in a legacy environment. Using a managed service allows the customer to realize significant cost savings through the reduction of _____.
Response:
A. Risk
B. Personnel
C. Security controls
D. Data
Answer: (SHOW ANSWER)

NEW QUESTION: 148
The different cloud service models have varying levels of responsibilities for functions and operations depending with the model's level of service.
In which of the following models would the responsibility for patching lie predominantly with the cloud customer?
A. DaaS
B. SaaS
C. PaaS
D. IaaS
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
With Infrastructure as a Service (IaaS), the cloud customer is responsible for deploying and maintaining its own systems and virtual machines. Therefore, the customer is solely responsible for patching and any other security updates it finds necessary. With Software as a Service (SaaS), Platform as a Service (PaaS), and Desktop as a Service (DaaS), the cloud provider maintains the infrastructure components and is responsible for maintaining and patching them.

NEW QUESTION: 149
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)
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: 150
Which type of testing tends to produce the best and most comprehensive results for discovering system vulnerabilities?
A. Dynamic
B. Pen
C. Static
D. Vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 151
Which of the cloud cross-cutting aspects relates to the requirements placed on the cloud provider by the cloud customer for minimum performance standards and requirements that must be met?
A. Regulatory requirements
B. SLAs
C. Auditability
D. Governance
Answer: B (LEAVE A REPLY)
Explanation
Whereas a contract spells out general terms and costs for services, the SLA is where the real meat of the business relationship and concrete requirements come into play. The SLA spells out in clear terms the minimum requirements for uptime, availability, processes, customer service and support, security controls and requirements, auditing and reporting, and potentially many other areas that define the business relationship and the success of it.

NEW QUESTION: 152
Which of the following can be useful for protecting cloud customers from a denial-of-service (DoS) attack against another customer hosted in the same cloud?
A. Reservations
B. Measured service
C. Limits
D. Shares
Answer: A (LEAVE A REPLY)
Explanation
Reservations ensure that a minimum level of resources will always be available to a cloud customer for them to start and operate their services. In the event of a DoS attack against one customer, they can guarantee that the other customers will still be able to operate.

NEW QUESTION: 153
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)
All the others are valid methods of data discovery; user-based is a red herring with no meaning.

NEW QUESTION: 154
Modern web service systems are designed for high availability and resiliency. Which concept pertains to the ability to detect problems within a system, environment, or application and programmatically invoke redundant systems or processes for mitigation?
A. Elasticity
B. Redundancy
C. Fault tolerance
D. Automation
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Fault tolerance allows a system to continue functioning, even with degraded performance, if portions of it fail or degrade, without the entire system or service being taken down. It can detect problems within a service and invoke compensating systems or functions to keep functionality going. Although redundancy is similar to fault tolerance, it is more focused on

having additional copies of systems available, either active or passive, that can take up services if one system goes down. Elasticity pertains to the ability of a system to resize to meet demands, but it is not focused on system failures. Automation, and its role in maintaining large systems with minimal intervention, is not directly related to fault tolerance.

NEW QUESTION: 155
Which of the following threat types involves an application that does not validate authorization for portions of itself beyond when the user first enters it?
A. Cross-site request forgery
B. Missing function-level access control
C. Injection
D. Cross-site scripting
Answer: (SHOW ANSWER)
Explanation/Reference:
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: 156
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. Motive
B. Public
C. Hybrid
D. Private
Answer: D (LEAVE A REPLY)

NEW QUESTION: 157
Which of the following roles involves the connection and integration of existing systems and services to a cloud environment?
A. Cloud service business manager

B. Cloud service user
C. Cloud service administrator
D. Cloud service integrator
Answer: (SHOW ANSWER)
The cloud service integrator is the official role that involves connecting and integrating existing systems and services with a cloud environment. This may involve moving services into a cloud environment, or connecting to external cloud services and capabilities from traditional data center-hosted services.

NEW QUESTION: 158
All of the following might be used as data discovery characteristics in a content-analysis-based data discovery effort except _____.
Response:
A. Pattern-matching
B. Keywords
C. Frequency
D. Inheritance
Answer: (SHOW ANSWER)

NEW QUESTION: 159
Which of the following are distinguishing characteristics of a managed service provider?
A. Be able to remotely monitor and manage objects for the customer and proactively maintain these objects under management.
B. Have some form of a help desk but no NOC.
C. Be able to remotely monitor and manage objects for the customer and reactively maintain these objects under management.
D. Have some form of a NOC but no help desk.
Answer: (SHOW ANSWER)
Explanation
According to the MSP Alliance, typically MSPs have the following distinguishing characteristics:
- Have some form of NOC service
- Have some form of help desk service
- Can remotely monitor and manage all or a majority of the objects for the customer
- Can proactively maintain the objects under management for the customer
- Can deliver these solutions with some form of predictable billing model, where the customer knows with great accuracy what her regular IT management expense will be

NEW QUESTION: 160
Which data sanitation method is also commonly referred to as "zeroing"?
A. Overwriting

B. Nullification
C. Blanking
D. Deleting
Answer: A (LEAVE A REPLY)
The zeroing of data--or the writing of null values or arbitrary data to ensure deletion has been fully completed--is officially referred to as overwriting. Nullification, deleting, and blanking are provided as distractor terms.

NEW QUESTION: 161
What concept does the "A" represent in the DREAD model?
A. Affected users
B. Authentication
C. Affinity
D. Authorization
Answer: A (LEAVE A REPLY)
Affected users refers to the percentage of users who would be impacted by a successful exploit.
Scoring ranges from 0, which means no users are impacted, to 10, which means all users are impacted.

NEW QUESTION: 162
All of the following are identity federation standards commonly found in use today except _____.
Response:
A. OAuth
B. PGP
C. OpenID
D. WS-Federation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 163
There is a large gap between the privacy laws of the United States and those of the European Union.
Bridging this gap is necessary for American companies to do business with European companies and in European markets in many situations, as the American companies are required to comply with the stricter requirements.
Which US program was designed to help companies overcome these differences?
A. SOX
B. HIPAA
C. GLBA
D. Safe Harbor

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

NEW QUESTION: 164
Which of the following jurisdictions lacks a comprehensive national policy on data privacy and the protection of personally identifiable information (PII)?
A. European Union
B. Asian-Pacific Economic Cooperation
C. United States
D. Russia
Answer: C (LEAVE A REPLY)
The United States has a myriad of regulations focused on specific types of data, such as healthcare and financial, but lacks an overall comprehensive privacy law on the national level. The European Union, the Asian- Pacific Economic Cooperation, and Russia all have national privacy protections and regulations for the handling the PII data of their citizens.

NEW QUESTION: 165
Which of the following is NOT a key area for performance monitoring as far as an SLA is concerned?
A. CPU
B. Users
C. Memory
D. Network
Answer: B (LEAVE A REPLY)
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: 166
Which of the following storage types is most closely associated with a traditional file system and tree structure?
A. Volume
B. Unstructured
C. Object
D. Structured
Answer: (SHOW ANSWER)
Explanation
Volume storage works as a virtual hard drive that is attached to a virtual machine. The operating system sees the volume the same as how a traditional drive on a physical server would be seen.

NEW QUESTION: 167
Which of the following service capabilities gives the cloud customer the least amount of control over configurations and deployments?
A. Platform
B. Infrastructure
C. Software
D. Desktop
Answer: C (LEAVE A REPLY)
Explanation
The software service capability gives the cloud customer a fully established application, where only minimal user configuration options are allowed.

NEW QUESTION: 168
What is the cloud service model in which the customer is responsible for administration of the OS?
A. QaaS
B. SaaS
C. PaaS

D. IaaS
Answer: D (LEAVE A REPLY)
Explanation
In IaaS, the cloud provider only owns the hardware and supplies the utilities. The customer is responsible for the OS, programs, and data. In PaaS and SaaS, the provider also owns the OS. There is no QaaS. That is a red herring.

NEW QUESTION: 169
Which phase of the cloud data lifecycle also typically entails the process of data classification?
Response:
A. Store
B. Create
C. Use
D. Archive
Answer: (SHOW ANSWER)

NEW QUESTION: 170
Halon is now illegal to use for data center fire suppression. What is the reason it was outlawed?
Response:
A. It causes undue damage to electronic systems.
B. It does not adequately suppress fires.
C. It can harm the environment.
D. It poses a threat to health and human safety when deployed.
Answer: (SHOW ANSWER)

NEW QUESTION: 171
Many aspects and features of cloud computing can make eDiscovery compliance more difficult or costly.
Which aspect of cloud computing would be the MOST complicating factor?
A. Measured service
B. Broad network access
C. Multitenancy
D. Portability
Answer: C (LEAVE A REPLY)
Explanation
With multitenancy, multiple customers share the same physical hardware and systems. With the nature of a cloud environment and how it writes data across diverse systems that are shared by others, the process of eDiscovery becomes much more complicated. Administrators cannot pull physical drives or easily isolate which data to capture. They not

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

NEW QUESTION: 172
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)
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: 173
The use of which of the following technologies will NOT require the security dependency of an operating system, other than its own?
A. Type 1 hypervisor
B. Management plane
C. Type 2 hypervisor
D. Virtual machine
Answer: (SHOW ANSWER)

NEW QUESTION: 174
What is the primary reason that makes resolving jurisdictional conflicts complicated?
A. Different technology standards
B. Costs
C. Language barriers

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

NEW QUESTION: 175
Which cloud service category offers the most customization options and control to the cloud customer?
A. IaaS
B. SaaS
C. DaaS
D. PaaS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 176
Which of the following is considered a technological control?
A. Firewall software
B. Firing personnel
C. Fireproof safe
D. Fire extinguisher
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A firewall is a technological control. The safe and extinguisher are physical controls and firing someone is an administrative control.

NEW QUESTION: 177
A virtual network interface card (NIC) exists at layer _____ of the OSI model.
Response:
A. 8
B. 4
C. 2
D. 6
Answer: C (LEAVE A REPLY)

NEW QUESTION: 178
Which OSI layer does IPsec operate at?
A. Network
B. transport

C. Application
D. Presentation
Answer: A (LEAVE A REPLY)
A major difference between IPsec and other protocols such as TLS is that IPsec operates at the Internet network layer rather than the application layer, allowing for complete end-to-end encryption of all communications and traffic.

NEW QUESTION: 179
Which of the following is a widely used tool for code development, branching, and collaboration?
A. GitHub
B. Maestro
C. Orchestrator
D. Conductor
Answer: (SHOW ANSWER)
Explanation
GitHub is an open source tool that developers leverage for code collaboration, branching, and versioning.

NEW QUESTION: 180
What must SOAP rely on for security since it does not provide security as a built-in capability?
A. Encryption
B. Tokenization
C. TLS
D. SSL
Answer: A (LEAVE A REPLY)
Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for data passing, and it must rely on the encryption of those data packages for security. TLS and SSL (before it was deprecated) represent two commons approaches to using encryption for protection of data transmissions. However, they are only two possible options and do not encapsulate the overall concept the question is looking for.
Tokenization, which involves the replacement of sensitive data with opaque values, would not be appropriate for use with SOAP because the actual data is needed by the services.

NEW QUESTION: 181
Why might an organization choose to comply with the ISO 27001 standard?
Response:
A. International acceptance
B. Price
C. Ease of implementation

D. Speed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 182
When crafting plans and policies for data archiving, we should consider all of the following, except:
A. Immediacy of the technology
B. Archive location
C. The format of the data
D. The backup process
Answer: C (LEAVE A REPLY)

NEW QUESTION: 183
In which cloud service model is the customer required to maintain the OS?
A. Iaas
B. CaaS
C. PaaS
D. SaaS
Answer: (SHOW ANSWER)
In IaaS, the service is bare metal, and the customer has to install the OS and the software; the customer then is responsible for maintaining that OS. In the other models, the provider installs and maintains the OS.

NEW QUESTION: 184
In a cloud environment, encryption should be used for all the following, except:
A. Secure sessions/VPN
B. Long-term storage of data
C. Near-term storage of virtualized images
D. Profile formatting
Answer: D (LEAVE A REPLY)
Explanation

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

NEW QUESTION: 185
As part of the auditing process, getting a report on the deviations between intended configurations and actual policy is often crucial for an organization.
What term pertains to the process of generating such a report?
A. Deficiencies
B. Findings
C. Gap analysis
D. Errors
Answer: C (LEAVE A REPLY)
Explanation
The gap analysis determines if there are any differences between the actual configurations in use on systems and the policies that govern what the configurations are expected or mandated to be. The other terms provided are all similar to the correct answer ("findings" in particular is often used to articulate deviations in configurations), but gap analysis is the official term used.

NEW QUESTION: 186
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: 187
You have been tasked by management to offload processing and validation of incoming encoded data from your application servers and their associated APIs. Which of the following would be the most appropriate device or software to consider?
A. Web application firewall
B. XML firewall
C. XML accelerator

D. Firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 188
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)
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: 189
Other than cost savings realized due to measured service, what is another facet of cloud computing that will typically save substantial costs in time and money for an organization in the event of a disaster?
A. Broad network access
B. Interoperability
C. Resource pooling
D. Portability
Answer: A (LEAVE A REPLY)
With a typical BCDR solution, an organization would need some number of staff to quickly travel to the location of the BCDR site to configure systems and applications for recovery. With a cloud environment, everything is done over broad network access, with no need (or even possibility) to travel to a remote site at any time.

NEW QUESTION: 190
An audit scope statement defines the limits and outcomes from an audit.
Which of the following would NOT be included as part of an audit scope statement?
A. Reports
B. Certification
C. Billing
D. Exclusions

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

NEW QUESTION: 191
Which United States law is focused on data related to health records and privacy?
A. Safe Harbor
B. SOX
C. GLBA
D. HIPAA
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The Health Insurance Portability and Accountability Act (HIPAA) requires the U.S. Federal Department of Health and Human Services to publish and enforce regulations pertaining to electronic health records and identifiers between patients, providers, and insurance companies. It is focused on the security controls and confidentiality of medical records, rather than the specific technologies used, so long as they meet the requirements of the regulations.

NEW QUESTION: 192
An SLA contains the official requirements for contract performance and satisfaction between the cloud provider and cloud customer. Which of the following would NOT be a component with measurable metrics and requirements as part of an SLA?
A. Network
B. Users
C. Memory
D. CPU
Answer: B (LEAVE A REPLY)
Explanation
Dealing with users or user access would not be an appropriate item for inclusion in an SLA specifically.
However, user access and user experience would be covered indirectly through other metrics. Memory, CPU, and network resources are all typically included within an SLA for availability and response times when dealing with any incidents.

NEW QUESTION: 193

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: A (LEAVE A REPLY)

NEW QUESTION: 194
What type of security threat is DNSSEC designed to prevent?
A. Account hijacking
B. Snooping
C. Spoofing
D. Injection
Answer: C (LEAVE A REPLY)
DNSSEC is designed to prevent the spoofing and redirection of DNS resolutions to rogue sites.

NEW QUESTION: 195
Which cloud deployment model is MOST likely to offer free or very cheap services to users?
A. Hybrid
B. Community
C. Public
D. Private
Answer: C (LEAVE A REPLY)
Explanation
Public clouds offer services to anyone, regardless of affiliation, and are the most likely to offer free services to users. Examples of public clouds with free services include iCloud, Dropbox, and OneDrive. Private cloud models are designed for specific customers and for their needs, and would not offer services to the public at large, for free or otherwise. A community cloud is specific to a group of similar organizations and would not offer free or widely available public services. A hybrid cloud model would not fit the specifics of the question.

NEW QUESTION: 196
Which of the following is a risk associated with manual patching especially in the cloud?
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: 197
Which of the following is NOT an application or utility to apply and enforce baselines on a system?
A. Chef
B. GitHub
C. Puppet
D. Active Directory
Answer: (SHOW ANSWER)
GitHub is an application for code collaboration, including versioning and branching of code trees.
It is not used for applying or maintaining system configurations.

NEW QUESTION: 198
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: (SHOW ANSWER)
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: 199

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

A. Cloud provider

B. The application

C. Their home organization

D. Third-party authentication system

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

With a federated identity system, a user will perform authentication with their home organization, and the application will accept the authentication tokens and user information from the identity provider in order to grant access. The purpose of a federated system is to allow users to authenticate from their home organization. Therefore, using the application or a third-party authentication system would be contrary to the purpose of a federated system because it necessitates the creation of additional accounts. The use of a cloud provider would not be relevant to the operations of a federated system.

NEW QUESTION: 200

Which of the following pertains to fire safety standards within a data center, specifically with their enormous electrical consumption?

A. NFPA

B. BICSI

C. IDCA

D. Uptime Institute

Answer: A (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 201

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

A. Test data in sandboxed environments

B. Authentication of privileged users

C. Enforcing least privilege

D. Secure remote access

Answer: (SHOW ANSWER)

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

NEW QUESTION: 202

Which of the following management risks can make an organization's cloud environment unviable?

A. VM sprawl

B. Insider trading

C. Hostile takeover

D. Improper personnel selection

Answer: (SHOW ANSWER)

NEW QUESTION: 203

What process entails taking sensitive data and removing the indirect identifiers from each data object so that the identification of a single entity would not be possible?

A. Tokenization

B. Encryption

C. Anonymization

D. Masking

Answer: (SHOW ANSWER)

Explanation

Anonymization is a type of masking, where indirect identifiers are removed from a data set to prevent the mapping back of data to an individual. Although masking refers to the overall approach of covering sensitive data, anonymization is the best answer here because it is more specific to exactly what is being asked.

Tokenization involves the replacement of sensitive data with a key value that can be matched back to the real value. However, it is not focused on indirect identifiers or preventing the matching to an individual.

Encryption refers to the overall process of protecting data via key pairs and protecting confidentiality.

NEW QUESTION: 204

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

A. Object

B. Unstructured

C. Volume

D. Structured

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 205

Which jurisdiction lacks specific and comprehensive privacy laws at a national or top level of legal authority?

A. European Union
B. Germany
C. Russia
D. United States
Answer: D (LEAVE A REPLY)
The United States lacks a single comprehensive law at the federal level addressing data security and privacy, but there are multiple federal laws that deal with different industries.

NEW QUESTION: 206
Which of the following is considered an administrative control?
A. Access control process
B. Keystroke logging
C. Biometric authentication
D. Door locks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 207
Which Common Criteria Evaluation Assurance Level (EAL) is granted to those products that are formally verified in terms of design and tested by an independent third party?
A. 1
B. 3
C. 5
D. 7
Answer: D (LEAVE A REPLY)

NEW QUESTION: 208
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: 209
The management plane is used to administer a cloud environment and perform administrative tasks across a variety of systems, but most specifically it's used with the hypervisors. What does the management plane typically leverage for this orchestration?
A. APIs

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

NEW QUESTION: 210
With a federated identity system, what does the identity provider send information to after a successful authentication?
A. Relying party
B. Service originator
C. Service relay
D. Service relay
Answer: A (LEAVE A REPLY)
Upon successful authentication, the identity provider sends an assertion with appropriate attributes to the relying party to grant access and assign appropriate roles to the user. The other terms provided are similar sounding to the correct term but are not actual components of a federated system.

NEW QUESTION: 211
Which of the following best describes SAML?
A. A standard used for directory synchronization
B. A standard for developing secure application management logistics
C. A standard for exchanging authentication and authorization data between security domains
D. A standard for exchanging usernames and passwords across devices
Answer: C (LEAVE A REPLY)

NEW QUESTION: 212
Which of the following would NOT be a reason to activate a BCDR strategy?
A. Staffing loss
B. Terrorism attack
C. Utility disruptions
D. Natural disaster
Answer: A (LEAVE A REPLY)
Explanation
The loss of staffing would not be a reason to declare a BCDR situation because it does not impact production operations or equipment, and the same staff would be needed for a BCDR situation.

NEW QUESTION: 213
Which technology can be useful during the "share" phase of the cloud data lifecycle to continue to protect data as it leaves the original system and security controls?
A. IPS
B. WAF
C. DLP
D. IDS
Answer: (SHOW ANSWER)
Data loss prevention (DLP) can be applied to data that is leaving the security enclave to continue to enforce access restrictions and policies on other clients and systems.

NEW QUESTION: 214
Of the following, which is probably the most significant risk in a managed cloud environment?
A. DDoS
B. Guest escape
C. Physical attack on the utility service lines
D. Management plane breach
Answer: D (LEAVE A REPLY)

NEW QUESTION: 215
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)
Explanation
Traditional security controls would not be able to restrict a user from printing something that they have the ability to access and read, but IRM solutions would allow for such a restriction. If a user has permissions to read a file, he can also copy the file or print it under traditional controls, and the ability to modify or write will give the user the ability to delete.

NEW QUESTION: 216
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: 217
What does the REST API use to protect data transmissions?
A. NetBIOS
B. VPN
C. Encapsulation
D. TLS
Answer: (SHOW ANSWER)
Explanation
Representational State Transfer (REST) uses TLS for communication over secured channels. Although REST also supports SSL, at this point SSL has been phased out due to vulnerabilities and has been replaced by TLS.

NEW QUESTION: 218
What is an experimental technology that is intended to create the possibility of processing encrypted data without having to decrypt it first?

A. Quantum-state
B. Polyinstantiation
C. Homomorphic
D. Gastronomic
Answer: C (LEAVE A REPLY)
Homomorphic encryption hopes to achieve that goal; the other options are terms that have almost nothing to do with encryption.

NEW QUESTION: 219
What type of identity system allows trust and verifications between the authentication systems of multiple organizations?
Response:
A. Bidirectional
B. Federated
C. Collaborative
D. Integrated
Answer: B (LEAVE A REPLY)

NEW QUESTION: 220
Which security concept is based on preventing unauthorized access to data while also ensuring that it is accessible to those authorized to use it?
A. Integrity
B. Availability
C. Confidentiality
D. Nonrepudiation
Answer: C (LEAVE A REPLY)
The main goal of confidentiality is to ensure that sensitive information is not made available or leaked to parties that should not have access to it, while at the same time ensuring that those with appropriate need and authorization to access it can do so in a manner commensurate with their needs and confidentiality requirements.

NEW QUESTION: 221
Which type of cloud model typically presents the most challenges to a cloud customer during the "destroy" phase of the cloud data lifecycle?
A. IaaS
B. DaaS
C. SaaS
D. PaaS
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

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

NEW QUESTION: 222
A cloud provider is looking to provide a higher level of assurance to current and potential cloud customers about the design and effectiveness of their security controls. Which of the following audit reports would the cloud provider choose as the most appropriate to accomplish this goal?
Response:
A. SOC 3
B. SOC 1
C. SAS-70
D. SOC 2
Answer: (SHOW ANSWER)

NEW QUESTION: 223
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
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: 224
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: 225
Identity and access management (IAM) is a security discipline that ensures which of the following?
A. That all users are properly authorized
B. That the right individual gets access to the right resources at the right time for the right reasons.
C. That all users are properly authenticated
D. That unauthorized users will get access to the right resources at the right time for the right reasons
Answer: B (LEAVE A REPLY)
Options A and C are also correct, but included in B, making B the best choice. D is incorrect, because we don't want unauthorized users gaining access.

NEW QUESTION: 226
In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?
Response:
A. All of the above
B. Administrative
C. Physical
D. Technological
Answer: (SHOW ANSWER)

NEW QUESTION: 227
Countermeasures for protecting cloud operations against internal threats include all of the following except:

A. Extensive and comprehensive training programs, including initial, recurring, and refresher sessions
B. Skills and knowledge testing
C. Hardened perimeter devices
D. Aggressive background checks
Answer: C (LEAVE A REPLY)
Explanation
Hardened perimeter devices are more useful at attenuating the risk of external attack.

NEW QUESTION: 228
Which of the following does NOT relate to the hiding of sensitive data from data sets?
A. Obfuscation
B. Federation
C. Masking
D. Anonymization
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Federation pertains to authenticating systems between different organizations.

NEW QUESTION: 229
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: 230
Your organization is considering a move to a cloud environment and is looking for certifications or audit reports from cloud providers to ensure adequate security controls and

processes. Which of the following is NOT a security certification or audit report that would be pertinent?

A. SOC Type 2

B. FIPS 140-2

C. FedRAMP

D. PCI DSS

Answer: B (LEAVE A REPLY)

NEW QUESTION: 231

All of the following entitles are required to use FedRAMP-accredited Cloud Service Providers except _____.

Response:

A. The CIA

B. The US post office

C. The Department of Homeland Security

D. Federal Express

Answer: (SHOW ANSWER)

NEW QUESTION: 232

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

A. ISO 31000:2009

B. ISO 27017

C. NIST 800-92

D. HIPAA

Answer: A (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 233

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

A. Injection

B. Missing function-level access control

C. Cross-site scripting

D. Cross-site request forgery

Answer: D (LEAVE A REPLY)

Explanation

Explanation:
A cross-site request forgery (CSRF) attack forces a client that a user has used to authenticate to an application to send forged requests under the user's own credentials to execute commands and requests that the application thinks are coming from a trusted client and user. Although this type of attack cannot be used to steal data directly because the attacker has no way of seeing the results of the commands, it does open other ways to compromise an application. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries.

NEW QUESTION: 234
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: 235
In the wake of many scandals with major corporations involving fraud and the deception of investors and regulators, which of the following laws was passed to govern accounting and financial records and disclosures?
A. GLBA
B. Safe Harbor
C. HIPAA
D. SOX
Answer: D (LEAVE A REPLY)
Explanation
The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and accounting errors.The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy. The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Safe Harbor program was

designed by the US government as a way for American companies to comply with European Union privacy laws.

NEW QUESTION: 236
Which of the following is NOT one of five principles of SOC Type 2 audits?
A. Privacy
B. Processing integrity
C. Financial
D. Security
Answer: C (LEAVE A REPLY)
Explanation
The SOC Type 2 audits include five principles: security, privacy, processing integrity, availability, and confidentiality.

NEW QUESTION: 237
Which of the following is a valid risk management metric?
A. KPI
B. KRI
C. SOC
D. SLA
Answer: B (LEAVE A REPLY)
KRI stands for key risk indicator. KRIs are the red flags if you will in the world of risk management. When these change, they indicate something is amiss and should be looked at quickly to determine if the change is minor or indicative of something important.

NEW QUESTION: 238
Hardening the operating system refers to all of the following except:
A. Limiting administrator access
B. Closing unused ports
C. Removing antimalware agents
D. Removing unnecessary services and libraries
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Removing antimalware agents. Hardening the operating system means making it more secure. Limiting administrator access, closing unused ports, and removing unnecessary services and libraries all have the potential to make an OS more secure. But removing antimalware agents would actually make the system less secure. If anything, antimalware agents should be added, not removed.

NEW QUESTION: 239

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

A. PCI DSS

B. FISMA

C. SOX

D. HIPAA

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The payment card industry data security standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry regulatory standard, not a governmental one.

NEW QUESTION: 240

What is a serious complication an organization faces from the perspective of compliance with international operations?

A. Different certifications

B. Multiple jurisdictions

C. Different capabilities

D. Different operational procedures

Answer: B (LEAVE A REPLY)

Explanation

When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, and many times they might be in contention with one other or not clearly applicable. These requirements can include the location of the users and the type of data they enter into systems, the laws governing the organization that owns the application and any regulatory requirements they may have, as well as the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which might be multiple jurisdictions as well.

NEW QUESTION: 241

Which component of ITIL pertains to planning, coordinating, executing, and validating changes and rollouts to production environments?

A. Release management

B. Availability management

C. Problem management

D. Change management

Answer: A (LEAVE A REPLY)

Explanation

Release management involves planning, coordinating, executing, and validating changes and rollouts to the production environment. Change management is a higher-level

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

NEW QUESTION: 242
With IaaS, what is responsible for handling the security and control over the volume storage space?
A. Management plane
B. Operating system
C. Application
D. Hypervisor
Answer: B (LEAVE A REPLY)
Volume storage is allocated via a LUN to a system and then treated the same as any traditional storage.
The operating system is responsible for formatting and securing volume storage as well as controlling all access to it. Applications, although they may use volume storage and have permissions to write to it, are not responsible for its formatting and security. Both a hypervisor and the management plane are outside of an individual system and are not responsible for managing the files and storage within that system.

NEW QUESTION: 243
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: (SHOW ANSWER)

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: 244
Which cloud storage type uses an opaque value or descriptor to categorize and organize data?
Response:
A. Structured
B. Unstructured
C. Volume
D. Object
Answer: (SHOW ANSWER)

NEW QUESTION: 245
Apart from using encryption at the file system level, what technology is the most widely used to protect data stored in an object storage system?
A. TLS
B. HTTPS
C. VPN
D. IRM
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Information rights management (IRM) technologies allow security controls and policies to be enforced on a data object regardless of where it resides. They also allow for extended controls such as expirations and copying restrictions, which are not available through traditional control mechanisms. 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 and likely will be used in conjunction with other object data protection strategies.

NEW QUESTION: 246
Which of the following would NOT be considered part of resource pooling with an Infrastructure as a Service implementation?

A. Storage
B. Application
C. Mamory
D. CPU
Answer: (SHOW ANSWER)
Explanation
Infrastructure as a Service pools the compute resources for platforms and applications to build upon, including CPU, memory, and storage. Applications are not part of an IaaS offering from the cloud provider.

NEW QUESTION: 247
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: 248
Many of the traditional concepts of systems and services for a traditional data center also apply to the cloud. Both are built around key computing concepts.
Which of the following compromise the two facets of computing?
A. CPU and software
B. CPU and storage
C. CPU and memory
D. Memory and networking
Answer: C (LEAVE A REPLY)
The CPU and memory resources of an environment together comprise its "computing" resources.
Cloud environments, especially public clouds, are enormous pools of resources for computing and are typically divided among a large number of customers with constantly changing needs and demands. Although storage and networking are core components of a cloud environment, they do not comprise its computing core. Software, much like within a

traditional data center, is highly subjective based on the application, system, service, or cloud computing model used; however, it is not one of the core cloud components.

NEW QUESTION: 249
Which format is the most commonly used standard for exchanging information within a federated identity system?
A. XML
B. HTML
C. SAML
D. JSON
Answer: C (LEAVE A REPLY)
Security Assertion Markup Language (SAML) is the most common data format for information exchange within a federated identity system. It is used to transmit and exchange authentication and authorization data.XML is similar to SAML, but it's used for general-purpose data encoding and labeling and is not used for the exchange of authentication and authorization data in the way that SAML is for federated systems. JSON is used similarly to XML, as a text-based data exchange format that typically uses attribute-value pairings, but it's not used for authentication and authorization exchange. HTML is used only for encoding web pages for web browsers and is not used for data exchange--and certainly not in a federated system.

NEW QUESTION: 250
Virtual machine (VM) configuration management (CM) tools should probably include _____.
Response:
A. Biometric recognition
B. Log file generation
C. Anti-tampering mechanisms
D. Hackback capabilities
Answer: B (LEAVE A REPLY)

NEW QUESTION: 251
Which of the following threat types involves an application that does not validate authorization for portions of itself beyond when the user first enters it?
A. Cross-site request forgery
B. Missing function-level access control
C. Injection
D. Cross-site scripting
Answer: B (LEAVE A REPLY)
It is imperative that applications do checks when each function or portion of the application is accessed to ensure that the user is properly authorized. Without continual checks each

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

NEW QUESTION: 252
If a cloud computing customer wishes to guarantee that a minimum level of resources will always be available, which of the following set of services would compromise the reservation?
A. Memory and networking
B. CPU and software
C. CPU and storage
D. CPU and memory
Answer: D (LEAVE A REPLY)
A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources.
A reservation pertains to memory and CPU resources. Under the concept of a reservation, memory and CPU are the guaranteed resources, but storage and networking are not included even though they are core components of cloud computing. Software would be out of scope for a guarantee and doesn't really pertain to the concept.

NEW QUESTION: 253
Why does a Type 1 hypervisor typically offer tighter security controls than a Type 2 hypervisor?
A. A Type 1 hypervisor also controls patching of its hosted virtual machines ensure they are always secure.
B. A Type 1 hypervisor is tied directly to the bare metal and only runs with code necessary to perform its specific mission.
C. A Type 1 hypervisor performs hardware-level encryption for tighter security and efficiency.
D. A Type 1 hypervisor only hosts virtual machines with the same operating systems as the hypervisor.
Answer: (SHOW ANSWER)
Explanation

Type 1 hypervisors run directly on top of the bare metal and only contain the code and functions required to perform their purpose. They do not rely on any other systems or contain extra features to secure.

NEW QUESTION: 254
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: D (LEAVE A REPLY)
Explanation
Dynamic resource scheduling (DRS) is used within all clustering systems as the method for clusters to provide high availability, scaling, management, and workload distribution and balancing of jobs and processes. From a physical infrastructure perspective, DRS is used to balance compute loads between physical hosts in a cloud to maintain the desired thresholds and limits on the physical hosts.

NEW QUESTION: 255
Designers making applications for the cloud have to take into consideration risks and operational constraints that did not exist or were not as pronounced in the legacy environment. Which of the following is an element cloud app designers may have to consider incorporating in software for the cloud that might not have been as important in the legacy environment?
A. IAM capability
B. Field validation
C. Encryption for data at rest and in motion
D. DDoS resistance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 256
Cloud systems are increasingly used for BCDR solutions for organizations.
What aspect of cloud computing makes their use for BCDR the most attractive?
A. On-demand self-service
B. Measured service
C. Portability
D. Broad network access
Answer: B (LEAVE A REPLY)
Business continuity and disaster recovery (BCDR) solutions largely sit idle until they are actually needed. This traditionally has led to increased costs for an organization because

physical hardware must be purchased and operational but is not used. By using a cloud system, an organization will only pay for systems when they are being used and only for the duration of use, thus eliminating the need for extra hardware and costs. Portability is the ability to easily move services among different cloud providers. Broad network access allows access to users and staff from anywhere and from different clients, and although this would be important for a BCDR situation, it is not the best answer in this case. On-demand self-service allows users to provision services automatically and when needed, and although this too would be important for BCDR situations, it is not the best answer because it does not address costs or the biggest benefits to an organization.

NEW QUESTION: 257
What type of PII is controlled based on laws and carries legal penalties for noncompliance with requirements?
A. Contractual
B. Regulated
C. Specific
D. Jurisdictional
Answer: B (LEAVE A REPLY)
Regulated PII involves those requirements put forth by specific laws or regulations, and unlike contractual PII, where a violation can lead to contractual penalties, a violation of regulated PII can lead to fines or even criminal charges in some jurisdictions. PII regulations can depend on either the jurisdiction that applies to the hosting location or application or specific legislation based on the industry or type of data used.

NEW QUESTION: 258
Which of the following could be used as a second component of multifactor authentication if a user has an RSA token?
A. Access card
B. USB thumb drive
C. Retina scan
D. RFID
Answer: (SHOW ANSWER)

A retina scan could be used in conjunction with an RSA token because it is a biometric factor, and thus a different type of factor. An access card, RFID, and USB thumb drive are all items in possession of a user, the same as an RSA token, and as such would not be appropriate.

NEW QUESTION: 259
What type of masking would you employ to produce a separate data set for testing purposes based on production data without any sensitive information?
A. Dynamic
B. Tokenized
C. Replicated
D. Static
Answer: (SHOW ANSWER)
Explanation
Static masking involves taking a data set and replacing sensitive fields and values with non-sensitive or garbage data. This is done to enable testing of an application against data that resembles production data, both in size and format, but without containing anything sensitive. Dynamic masking involves the live and transactional masking of data while an application is using it. Tokenized would refer to tokenization, which is the replacing of sensitive data with a key value that can later be matched back to the original value, and although it could be used as part of the production of test data, it does not refer to the overall process.
Replicated is provided as an erroneous answer, as replicated data would be identical in value and would not accomplish the production of a test set.

NEW QUESTION: 260
Which of the cloud deployment models involves spanning multiple cloud environments or a mix of cloud hosting models?
A. Community
B. Public
C. Hybrid
D. Private
Answer: (SHOW ANSWER)
A hybrid cloud model involves the use of more than one type of cloud hosting models, typically the mix of private and public cloud hosting models.

NEW QUESTION: 261
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: 262
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?
Response:
A. System vulnerabilities
B. Data loss
C. Insecure interfaces
D. Account hijacking
Answer: B (LEAVE A REPLY)

NEW QUESTION: 263
Which of the following are attributes of cloud computing?
A. Minimal management effort and shared resources
B. High cost and unique resources
C. Rapid provisioning and slow release of resources
D. Limited access and service provider interaction
Answer: A (LEAVE A REPLY)
Explanation
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NEW QUESTION: 264
Which of the following is not a factor an organization might use in the cost-benefit analysis when deciding whether to migrate to a cloud environment?
Response:
A. The time savings and efficiencies offered by the cloud service
B. Branding associated with which cloud provider might be selected

C. Shifting from capital expenditures to support IT investment to operational expenditures
D. Pooled resources in the cloud
Answer: B (LEAVE A REPLY)

NEW QUESTION: 265
_____ is the legal concept whereby a cloud customer is held to a reasonable expectation for providing security of its users' and clients' privacy data.
Response:
A. Due diligence
B. Due care
C. Reciprocity
D. Liability
Answer: (SHOW ANSWER)

NEW QUESTION: 266
Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?
A. Regulation
B. Multitenancy
C. Virtualization
D. Resource pooling
Answer: B (LEAVE A REPLY)
With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers. Especially within a public cloud model, it is not possible or practical for a cloud provider to alter its services for specific customer demands.
Resource pooling and virtualization within a cloud environment would be the same for all customers, and would not impact certifications that a cloud provider might be willing to pursue. Regulations would form the basis for certification problems and would be a reason for a cloud provider to pursue specific certifications to meet customer requirements.

NEW QUESTION: 267
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. Insecure interfaces
B. System vulnerabilities
C. Data loss
D. Account hijacking
Answer: C (LEAVE A REPLY)

NEW QUESTION: 268
Which type of testing uses the same strategies and toolsets that hackers would use?
A. Static
B. Malicious
C. Penetration
D. Dynamic
Answer: C (LEAVE A REPLY)
Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discovery potential vulnerabilities. Although the term malicious captures much of the intent of penetration testing from the perspective of an attacker, it is not the best answer. Static and dynamic are two types of system testing--where static is done offline and with knowledge of the system, and dynamic is done on a live system without any previous knowledge is associated--but neither describes the type of testing being asked for in the question.

NEW QUESTION: 269
When considering the option to migrate from an on-premises environment to a hosted cloud service, an organization should weigh the risks of allowing external entities to access the cloud data for collaborative purposes against _____.
A. Disclosing the data publicly
B. Not securing the data in the legacy environment
C. Sending the data outside the legacy environment for collaborative purposes
D. Inviting external personnel into the legacy workspace in order to enhance collaboration
Answer: C (LEAVE A REPLY)

NEW QUESTION: 270
Which of the following is NOT something that an HIDS will monitor?
A. Configurations
B. User logins
C. Critical system files
D. Network traffic
Answer: (SHOW ANSWER)
Explanation
A host intrusion detection system (HIDS) monitors network traffic as well as critical system files and configurations.

NEW QUESTION: 271
Which of the following cloud aspects complicates eDiscovery?
A. Resource pooling
B. On-demand self-service
C. Multitenancy

D. Measured service
Answer: C (LEAVE A REPLY)
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: 272
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. Federal law prohibits it in the United States.
B. Cloud data storage may not be affected by degaussing.
C. The blast radius is too wide.
D. All the data storage space in the cloud is already gaussed.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 273
What is the intellectual property protection for the logo of a new video game?
Response:
A. Trade secret
B. Trademark
C. Patent
D. Copyright
Answer: (SHOW ANSWER)

NEW QUESTION: 274
What are the six components that make up the STRIDE threat model?
Response:

A. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
B. Spoofing, Tampering, Repudiation, Information Disclosure, Distributed Denial of Service, and Elevation of Privilege
C. Spoofing, Tampering, Non-Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
D. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Social Engineering
Answer: (SHOW ANSWER)

NEW QUESTION: 275
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
Which of these activities should you perform before deploying the tool?
A. Adjust the hypervisors
B. Reconstruct your firewalls
C. Survey your company's departments about the data under their control
D. Harden all your routers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 276
What concept does the "I" represent with the STRIDE threat model?
A. Integrity
B. Information disclosure
C. IT security
D. Insider threat
Answer: B (LEAVE A REPLY)
Perhaps the biggest concern for any user is having their personal and sensitive information disclosed by an application. There are many aspects of an application to consider with security and protecting this information, and it is very difficult for any application to fully ensure security from start to finish. The obvious focus is on security within the application itself, as well as protecting and storing the data.

NEW QUESTION: 277
Which type of web application monitoring most closely measures actual activity?
Response:
A. Synthetic performance monitoring
B. Real-user monitoring (RUM)
C. Database application monitor (DAM)
D. Security information and event management (SIEM)
Answer: (SHOW ANSWER)

NEW QUESTION: 278
Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?
A. SOC 1
B. SOC 2
C. SOC 3
D. SOC 4
Answer: B (LEAVE A REPLY)
Explanation
SOC 2 deals with the CIA triad. SOC 1 is for financial reporting. SOC 3 is only an attestation by the auditor.
There is no SOC 4.

NEW QUESTION: 279
An audit against the _____ will demonstrate that an organization has -adequate security controls to meet its ISO 27001 requirements.
Response:
A. SSAE 16 standard
B. ISO 27002 certification criteria
C. SAS 70 standard
D. NIST SP 800-53
Answer: (SHOW ANSWER)

NEW QUESTION: 280
SOX was enacted because of which of the following?
A. All of the above
B. Poor financial controls
C. Poor BOD oversight
D. Lack of independent audits
Answer: A (LEAVE A REPLY)

NEW QUESTION: 281
Which of the following would be considered an example of insufficient due diligence leading to security or operational problems when moving to a cloud?
A. Monitoring
B. Use of a remote key management system
C. Programming languages used
D. Reliance on physical network controls
Answer: D (LEAVE A REPLY)
Explanation

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

NEW QUESTION: 282
Which United States law is focused on PII as it relates to the financial industry?
A. HIPAA
B. SOX
C. Safe Harbor
D. GLBA
Answer: (SHOW ANSWER)
Explanation
The GLBA, as it is commonly called based on the lead sponsors and authors of the act, is officially known as
"The Financial Modernization Act of 1999." It is specifically focused on PII as it relates to financial institutions. There are three specific components of it, covering various areas and use, on top of a general requirement that all financial institutions must provide all users and customers with a written copy of their privacy policies and practices, including with whom and for what reasons their information may be shared with other entities.

NEW QUESTION: 283
Why does a Type 2 hypervisor typically offer less security control than a Type 1 hypervisor?
A. A Type 2 hypervisor runs on top of another operating system and is dependent on the security of the OS for its own security.
B. A Type 2 hypervisor allows users to directly perform some functions with their own access.
C. A Type 2 hypervisor is open source, so attackers can more easily find exploitable vulnerabilities with that access.
D. A Type 2 hypervisor is always exposed to the public Internet for federated identity access.
Answer: (SHOW ANSWER)
A Type 2 hypervisor differs from a Type 1 hypervisor in that it runs on top of another operating system rather than directly tied into the underlying hardware of the virtual host servers. With this type of implementation, additional security and architecture concerns come into play because the interaction between the operating system and the hypervisor

becomes a critical link. The hypervisor no longer has direct interaction and control over the underlying hardware, which means that some performance will be lost due to the operating system in the middle needing its own resources, patching requirements, and operational oversight.

NEW QUESTION: 284
When a customer performs a penetration test in the cloud, why isn't the test an optimum simu-lation of attack conditions?
Response:
A. Advanced notice removes the element of surprise
B. Attackers don't use remote access for cloud activity
C. When cloud customers use malware, it's not the same as when attackers use malware
D. Regulator involvement changes the attack surface
Answer: (SHOW ANSWER)

NEW QUESTION: 285
Which of the following threat types involves an application developer leaving references to internal information and configurations in code that is exposed to the client?
A. Sensitive data exposure
B. Security misconfiguration
C. Insecure direct object references
D. Unvalidated redirect and forwards
Answer: C (LEAVE A REPLY)
An insecure direct object reference occurs when a developer has in their code a reference to something on the application side, such as a database key, the directory structure of the application, configuration information about the hosting system, or any other information that pertains to the workings of the application that should not be exposed to users or the network. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, allowing spoofing for malware of phishing attacks. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data.
Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner.

NEW QUESTION: 286
Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?
A. Hybrid
B. Public
C. Private

D. Community
Answer: (SHOW ANSWER)
Explanation
Popular services such as iCloud, Dropbox, and OneDrive are all publicly available and are open to any user for free, with possible add-on services offered for a cost.

NEW QUESTION: 287
Which process serves to prove the identity and credentials of a user requesting access to an application or data?
A. Repudiation
B. Authentication
C. Identification
D. Authorization
Answer: (SHOW ANSWER)
Authentication is the process of proving whether the identity presented by a user is true and valid. This can be done through common mechanisms such as user ID and password combinations or with more secure methods such as multifactor authentication.

NEW QUESTION: 288
Which of the following service capabilities gives the cloud customer the most control over resources and configurations?
A. Desktop
B. Platform
C. Infrastructure
D. Software
Answer: C (LEAVE A REPLY)
Explanation
The infrastructure service capability gives the cloud customer substantial control in provisioning and configuring resources, including processing, storage, and network resources.

NEW QUESTION: 289

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

NEW QUESTION: 290
Typically, SSDs are _____.
Response:
A. More expensive than spinning platters
B. Heavier than tape libraries
C. Larger than tape backup
D. More subject to malware than legacy drives
Answer: (SHOW ANSWER)

NEW QUESTION: 291
Which aspect of cloud computing will be most negatively impacted by vendor lock-in?
A. Elasticity
B. Reversibility
C. Interoperability
D. Portability
Answer: (SHOW ANSWER)
Explanation
A cloud customer utilizing proprietary APIs or services from one cloud provider that are unlikely to be available from another cloud provider will most negatively impact portability.

NEW QUESTION: 292
When using an IaaS solution, what is a key benefit provided to the customer?
A. Metered and priced on the basis of units consumed
B. Increased energy and cooling system efficiencies
C. Transferred cost of ownership
D. The ability to scale up infrastructure services based on projected usage
Answer: A (LEAVE A REPLY)
IaaS has a number of key benefits for organizations, which include but are not limited to these: --
- Usage is metered and priced on the basis of units (or instances) consumed. This can also be billed back to specific departments or functions.

- It has an ability to scale up and down infrastructure services based on actual usage. This is particularly useful and beneficial where there are significant spikes and dips within the usage curve for infrastructure.
- It has a reduced cost of ownership. There is no need to buy assets for everyday use, no loss of asset value over time, and reduced costs of maintenance and support.
- It has a reduced energy and cooling costs along with "green IT" environment effect with optimum use of IT resources and systems.

NEW QUESTION: 293
Which security concept would business continuity and disaster recovery fall under?
A. Confidentiality
B. Availability
C. Fault tolerance
D. Integrity
Answer: B (LEAVE A REPLY)
Disaster recovery and business continuity are vital concerns with availability. If data is destroyed or compromised, having regular backup systems in place as well as being able to perform disaster recovery in the event of a major or widespread problem allows operations to continue with an acceptable loss of time and data to management. This also ensures that sensitive data is protected and persisted in the event of the loss or corruption of data systems or physical storage systems.

NEW QUESTION: 294
Which of the following may unilaterally deem a cloud hosting model inappropriate for a system or application?
A. Multitenancy
B. Certification
C. Regulation
D. Virtualization
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Some regulations may require specific security controls or certifications be used for hosting certain types of data or functions, and in some circumstances they may be requirements that are unable to be met by any cloud provider.

NEW QUESTION: 295
To address shared monitoring and testing responsibilities in a cloud configuration, the provider might offer all these to the cloud customer except:
A. Access to audit logs and performance data
B. DLP solution results

C. Security control administration
D. SIM, SEIM. and SEM logs
Answer: (SHOW ANSWER)
Explanation
Explanation:
While the provider might share any of the other options listed, the provider will not share administration of security controls with the customer. Security controls are the sole province of the provider.

NEW QUESTION: 296
If a key feature of cloud computing that your organization desires is the ability to scale and expand without limit or concern about available resources, which cloud deployment model would you MOST likely be considering?
A. Public
B. Hybrid
C. Private
D. Community
Answer: A (LEAVE A REPLY)
Public clouds, such as AWS and Azure, are massive systems run by major corporations, and they account for a significant share of Internet traffic and services. They are always expanding, offer enormous resources to customers, and are the least likely to run into resource constraints compared to the other deployment models.
Private clouds would likely have the resources available for specific uses and could not be assumed to have a large pool of resources available for expansion. A community cloud would have the same issues as a private cloud, being targeted to similar organizations. A hybrid cloud, because it spans multiple clouds, would not fit the bill either, without the use of individual cloud models.

NEW QUESTION: 297
Without the extensive funds of a large corporation, a small-sized company could gain considerable and cost-effective services for which of the following concepts by moving to a cloud environment?
A. Regulatory
B. Security
C. Testing
D. Development
Answer: B (LEAVE A REPLY)
Explanation
Cloud environments, regardless of the specific deployment model used, have extensive and robust security controls in place, especially in regard to physical and infrastructure security. A small company can leverage the extensive security controls and monitoring

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

NEW QUESTION: 298
Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations. Which of the following is NOT a regulatory system from the United States federal government?
A. HIPAA
B. SOX
C. FISMA
D. PCI DSS
Answer: D (LEAVE A REPLY)
The Payment Card Industry Data Security Standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry-regulatory standard, not a governmental one. The Sarbanes-Oxley Act (SOX) was passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders. The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

NEW QUESTION: 299
When an organization is considering the use of cloud services for BCDR planning and solutions, which of the following cloud concepts would be the most important?
A. Reversibility
B. Elasticity
C. Interoperability
D. Portability
Answer: D (LEAVE A REPLY)
Portability is the ability for a service or system to easily move among different cloud providers. This is essential for using a cloud solution for BCDR because vendor lock-in would inhibit easily moving and setting up services in the event of a disaster, or it would necessitate a large number of configuration or component changes to implement. Interoperability, or the ability to reuse components for other services or systems, would not be an important factor for BCDR. Reversibility, or the ability to remove all data quickly and completely from a cloud environment, would be important at the end of a disaster, but

would not be important during setup and deployment. Elasticity, or the ability to resize resources to meet current demand, would be very beneficial to a BCDR situation, but not as vital as portability.

NEW QUESTION: 300
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: (SHOW ANSWER)
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: 301
Which aspect of security is DNSSEC designed to ensure?
A. Integrity
B. Authentication
C. Availability
D. Confidentiality
Answer: A (LEAVE A REPLY)
DNSSEC is a security extension to the regular DNS protocol and services that allows for the validation of the integrity of DNS lookups. It does not address confidentiality or availability at all. It allows for a DNS client to perform DNS lookups and validate both their origin and authority via the cryptographic signature that accompanies the DNS response.

NEW QUESTION: 302
Single sign-on systems work by authenticating users from a centralized location or using a centralized method, and then allowing applications that trust the system to grant those

users access. What would be passed between the authentication system and the applications to grant a user access?
A. Certificate
B. Token
C. Credential
D. Ticket
Answer: B (LEAVE A REPLY)

NEW QUESTION: 303
For optimal security, trust zones are used for network segmentation and isolation. They allow for the separation of various systems and tiers, each with its own security level. Which of the following is typically used to allow administrative personnel access to trust zones?
A. IPSec
B. SSH
C. VPN
D. TLS
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Virtual private networks (VPNs) are used to provide administrative personnel with secure communication channels through security systems and into trust zones. They allow staff who perform system administration tasks to have access to ports and systems that are not allowed from the public Internet.
IPSec is an encryption protocol for point-to-point communications at the network level, and may be used within a trust zone but not to give access into a trust zone. TLS enables encryption of communications between systems and services and would likely be used to secure the VPN communications, but it does not represent the overall concept being asked for in the question. SSH allows for secure shell access to systems, but not for general access into trust zones.

NEW QUESTION: 304
Why are PaaS environments at a higher likelihood of suffering backdoor vulnerabilities?
A. They are often used for software development.
B. They are scalable.
C. They have multitenancy.
D. They rely on virtualization.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 305

Which of the following is NOT considered a type of data loss?
A. Data corruption
B. Stolen by hackers
C. Accidental deletion
D. Lost or destroyed encryption keys
Answer: B (LEAVE A REPLY)
Explanation
The exposure of data by hackers is considered a data breach. Data loss focuses on the data availability rather than security. Data loss occurs when data becomes lost, unavailable, or destroyed, when it should not have been.

NEW QUESTION: 306
Which of the following types of software is a Type 2 hypervisor dependent on that a Type 1 hypervisor isn't?
Response:
A. VPN
B. Firewall
C. Operating system
D. IDS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 307
What is a serious complication an organization faces from the compliance perspective with international operations?
A. Multiple jurisdictions
B. Different certifications
C. Different operational procedures
D. Different capabilities
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, which often may not be clearly applicable or may be in contention with each other. These requirements can involve the location of the users and the type of data they enter into systems, the laws governing the organization that owns the application and any regulatory requirements they may have, and finally the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which may be multiple jurisdictions as well. Different certifications would not come into play as a challenge because the major IT and data center certifications are international and would apply to any cloud provider. Different capabilities and different operational procedures would be mitigated by the organization's selection of a cloud

provider and would not be a challenge if an appropriate provider was chosen, regardless of location.

NEW QUESTION: 308
Which of the following areas of responsibility always falls completely under the purview of the cloud provider, regardless of which cloud service category is used?
A. Infrastructure
B. Data
C. Physical
D. Governance
Answer: C (LEAVE A REPLY)
Regardless of the cloud service category used, the physical environment is always the sole responsibility of the cloud provider. In many instances, the cloud provider will supply audit reports or some general information about their physical security practices, especially to those customers or potential customers that may have regulatory requirements, but otherwise the cloud customer will have very little insight into the physical environment. With IaaS, the infrastructure is a shared responsibility between the cloud provider and cloud customer. With all cloud service categories, the data and governance are always the sole responsibility of the cloud customer.

NEW QUESTION: 309
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)
Print spooling is not a metric for system performance; all the rest are.

NEW QUESTION: 310
In a federated identity arrangement using a trusted third-party model, who is the identity provider and who is the relying party?
A. The users of the various organizations within the federations within the federation/a CASB
B. Each member organization/a trusted third party
C. Each member organization/each member organization
D. A contracted third party/the various member organizations of the federation
Answer: D (LEAVE A REPLY)
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: 311
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)
Explanation
When we gather information about business requirements, we need to do a complete inventory, receive accurate valuation of assets (usually from the owners of those assets), and assess criticality; this collection of information does not tell us, objectively, how useful an asset is, however.

NEW QUESTION: 312
Setting thermostat controls by measuring the temperature will result in the _____ highest energy costs.
Response:
A. Return air
B. Under-floor
C. Server inlet
D. External ambient
Answer: A (LEAVE A REPLY)

NEW QUESTION: 313
Which security concept is focused on the trustworthiness of data?
A. Integrity
B. Availability
C. Nonrepudiation
D. Confidentiality
Answer: A (LEAVE A REPLY)
Explanation
Integrity is focused on the trustworthiness of data as well as the prevention of unauthorized modification or tampering of it. A prime consideration for maintaining integrity is an emphasis on the change management and configuration management aspects of operations, so that all modifications are predictable, tracked, logged, and verified, whether they are performed by actual human users or systems processes and scripts.

NEW QUESTION: 314
What is the biggest benefit to leasing space in a data center versus building or maintain your own?
A. Certification
B. Costs
C. Regulation
D. Control
Answer: B (LEAVE A REPLY)
Explanation
When leasing space in a data center, an organization can avoid the enormous startup and building costs associated with a data center, and can instead leverage economies of scale by grouping with other organizations and sharing costs.

NEW QUESTION: 315
What does SDN stand for within a cloud environment?
A. Software-dynamic networking
B. Software-defined networking
C. Software-dependent networking
D. System-dynamic nodes
Answer: B (LEAVE A REPLY)
Explanation
Software-defined networking separates the administration of network filtering and network forwarding to allow for distributed administration.

NEW QUESTION: 316
During the assessment phase of a risk evaluation, what are the two types of tests that are performed?
Response:
A. Technical and managerial
B. Physical and logical
C. Internal and external
D. Qualitative and quantitative
Answer: D (LEAVE A REPLY)

NEW QUESTION: 317
What is the biggest challenge to data discovery in a cloud environment?
A. Format
B. Ownership
C. Location
D. Multitenancy
Answer: C (LEAVE A REPLY)
With the distributed nature of cloud environments, the foremost challenge for data discovery is awareness of the location of data and keeping track of it during the constant motion of cloud storage systems.

NEW QUESTION: 318
Which type of audit report is considered a "restricted use" report for its intended audience?
A. SAS-70
B. SSAE-16
C. SOC Type 1
D. SOC Type 2
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
SOC Type 1 reports are considered "restricted use" reports. They are intended for management and stakeholders of an organization, clients of the service organization, and auditors of the organization. They are not intended for release beyond those audiences.

NEW QUESTION: 319
With the rapid emergence of cloud computing, very few regulations were in place that pertained to it specifically, and organizations often had to resort to using a collection of regulations that were not specific to cloud in order to drive audits and policies.
Which standard from the ISO/IEC was designed specifically for cloud computing?
A. ISO/IEC 27001
B. ISO/IEC 19889
C. ISO/IEC 27001:2015
D. ISO/IEC 27018
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:

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

NEW QUESTION: 320
Just like the risk management process, the BCDR planning process has a defined sequence of steps and processes to follow to ensure the production of a comprehensive and successful plan.
Which of the following is the correct sequence of steps for a BCDR plan?
A. Define scope, gather requirements, assess risk, implement
B. Define scope, gather requirements, implement, assess risk
C. Gather requirements, define scope, implement, assess risk
D. Gather requirements, define scope, assess risk, implement
Answer: A (LEAVE A REPLY)
Explanation
The correct sequence for a BCDR plan is to define the scope, gather requirements based on the scope, assess overall risk, and implement the plan. The other sequences provided are not in the correct order.

NEW QUESTION: 321
From a security perspective, what component of a cloud computing infrastructure represents the biggest concern?
A. Hypervisor
B. Management plane
C. Object storage
D. Encryption
Answer: B (LEAVE A REPLY)
The management plane will have broad administrative access to all host systems throughout an environment; as such, it represents the most pressing security concerns. A compromise of the management plane can directly lead to compromises of any other systems within the environment. Although hypervisors represent a significant security concern to an environment because their compromise would expose any virtual systems hosted within them, the management plane is a better choice in this case because it controls multiple hypervisors. Encryption and object storage both represent lower-level security concerns.

NEW QUESTION: 322
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)
Explanation
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: 323
Security best practices in a virtualized network environment would include which of the following?
Response:
A. Hardening all outward-facing firewalls in order to make them resistant to attack
B. Using distinct ports and port groups for various VLANs on a virtual switch rather than running them through the same port
C. Running iSCSI traffic unencrypted in order to have it observed and monitored by NIDS
D. Adding HIDS to all virtual guests
Answer: B (LEAVE A REPLY)

NEW QUESTION: 324
What type of masking strategy involves replacing data on a system while it passes between the data and application layers?
A. Dynamic
B. Static
C. Replication
D. Duplication
Answer: (SHOW ANSWER)
Explanation
With dynamic masking, production environments are protected with the masking process being implemented between the application and data layers of the application. This allows for a masking translation to take place live in the system and during normal application processing of data.

NEW QUESTION: 325
Which of the following is a commonly used tool for maintaining system configurations?
A. Maestro
B. Orchestrator
C. Puppet
D. Conductor

Answer: (SHOW ANSWER)
Puppet is a commonly used tool for maintaining system configurations based on policies, and done so from a centralized authority.

NEW QUESTION: 326
What is a data custodian responsible for?
A. Customer access and alerts for all data
B. Data content, context, and associated business rules
C. Logging and alerts for all data
D. The safe custody, transport, storage of the data, and implementation of business rules
Answer: D (LEAVE A REPLY)

NEW QUESTION: 327
In the cloud motif, the data processor is usually:
A. The cloud customer
B. The cloud provider
C. The cloud access security broker
D. The party that assigns access rights
Answer: B (LEAVE A REPLY)
In legal terms, when "data processor" is defined, it refers to anyone who stores, handles, moves, or manipulates data on behalf of the data owner or controller. In the cloud computing realm, this is the cloud provider.

NEW QUESTION: 328
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: (SHOW ANSWER)
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: 329

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: (SHOW ANSWER)

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: 330

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

A. Adding encryption modules

B. Implementing certificate validations

C. Additional DNS lookups

D. No changes are needed.

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 331

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

A. Static

B. Malicious

C. Penetration

D. Dynamic

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

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

NEW QUESTION: 332
Which security certification serves as a general framework that can be applied to any type of system or application?
A. NIST SP 800-53
B. PCI DSS
C. ISO/IEC 27001
D. FIPS 140-2
Answer: C (LEAVE A REPLY)

NEW QUESTION: 333
Which component of ITIL involves planning for the restoration of services after an unexpected outage or incident?
A. Continuity management
B. Problem management
C. Configuration management
D. Availability management
Answer: A (LEAVE A REPLY)
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: 334
What's a potential problem when object storage versus volume storage is used within IaaS for application use and dependency?
A. Object storage is only optimized for small files.
B. Object storage is its own system, and data consistency depends on replication.
C. Object storage may have availability issues.

D. Object storage is dependent on access control from the host server.

Answer: B (LEAVE A REPLY)

Object storage runs on its own independent systems, which have their own redundancy and distribution.

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

NEW QUESTION: 335

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: 336

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

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

A. Packet

B. Payload

C. Object

D. Envelope

Answer: (SHOW ANSWER)

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: 337

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

A. Full inventory

B. Criticality

C. Value

D. Usefulness

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

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

NEW QUESTION: 338

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: (SHOW ANSWER)

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: 339

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

A. Public

B. Community

C. Hybrid

D. Private

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

NEW QUESTION: 340
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:
Response:
A. Tokenization
B. Obfuscation
C. Masking
D. Data discovery
Answer: D (LEAVE A REPLY)

NEW QUESTION: 341
Countermeasures for protecting cloud operations against external attackers include all of the following except:
A. Continual monitoring for anomalous activity.
B. Detailed and extensive background checks.
C. Regular and detailed configuration/change management activities
D. Hardened devices and systems, including servers, hosts, hypervisors, and virtual machines.
Answer: B (LEAVE A REPLY)
Background checks are controls for attenuating potential threats from internal actors; external threats aren't likely to submit to background checks.

NEW QUESTION: 342
When using transparent encryption of a database, where does the encryption engine reside?
Response:
A. At the application using the database
B. Within the database
C. In a key management system
D. On the instance(s) attached to the volume
Answer: B (LEAVE A REPLY)

NEW QUESTION: 343

Which of the following data sanitation methods would be the MOST effective if you needed to securely remove data as quickly as possible in a cloud environment?

A. Zeroing

B. Cryptographic erasure

C. Degaussing

D. Overwriting

Answer: B (LEAVE A REPLY)

NEW QUESTION: 344

Which of the following does NOT relate to the hiding of sensitive data from data sets?

A. Obfuscation

B. Federation

C. Masking

D. Anonymization

Answer: (SHOW ANSWER)

Explanation

Federation pertains to authenticating systems between different organizations.

NEW QUESTION: 345

Which of the following areas of responsibility would be shared between the cloud customer and cloud provider within the Software as a Service (SaaS) category?

A. Data

B. Governance

C. Application

D. Physical

Answer: C (LEAVE A REPLY)

With SaaS, the application is a shared responsibility between the cloud provider and cloud customer. Although the cloud provider is responsible for deploying, maintaining, and securing the application, the cloud customer does carry some responsibility for the configuration of users and options. Regardless of the cloud service category used, the physical environment is always the sole responsibility of the cloud provider. With all cloud service categories, the data and governance are always the sole responsibility of the cloud customer.

NEW QUESTION: 346

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

A. Cloud service integrator

B. Cloud service business manager

C. Cloud service user

D. Cloud service administrator

Answer: D (LEAVE A REPLY)
Explanation
The cloud service administrator is responsible for testing cloud services, monitoring services, administering security for services, providing usage reports on cloud services, and addressing problem reports

NEW QUESTION: 347
The tasks performed by the hypervisor in the virtual environment can most be likened to the tasks of the _____ in the legacy environment.
A. Central processing unit (CPU)
B. Security team
C. OS
D. PGP
Answer: (SHOW ANSWER)

NEW QUESTION: 348
What type of storage structure does object storage employ to maintain files?
A. Directory
B. Hierarchical
C. tree
D. Flat
Answer: (SHOW ANSWER)
Explanation
Explanation:
Object storage uses a flat file system to hold storage objects; it assigns files a key value that is then used to access them, rather than relying on directories or descriptive filenames. Typical storage layouts such as tree, directory, and hierarchical structures are used within volume storage, whereas object storage maintains a flat structure with key values.

NEW QUESTION: 349

Digital investigations have adopted many of the same methodologies and protocols as other types of criminal or scientific inquiries.
What term pertains to the application of scientific norms and protocols to digital investigations?
A. Scientific
B. Investigative
C. Methodological
D. Forensics
Answer: D (LEAVE A REPLY)
Forensics refers to the application of scientific methods and protocols to the investigation of crimes. Although forensics has traditionally been applied to well-known criminal proceedings and investigations, the term equally applies to digital investigations and methods. Although the other answers provide similar-sounding terms and ideas, none is the appropriate answer in this case.

NEW QUESTION: 350
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?
Response:
A. Token
B. Credential
C. Ticket
D. Certificate
Answer: A (LEAVE A REPLY)

NEW QUESTION: 351
Which format is the most commonly used standard for exchanging information within a federated identity system?
A. XML
B. HTML
C. SAML
D. JSON
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Security Assertion Markup Language (SAML) is the most common data format for information exchange within a federated identity system. It is used to transmit and exchange authentication and authorization data.XML is similar to SAML, but it's used for

general-purpose data encoding and labeling and is not used for the exchange of authentication and authorization data in the way that SAML is for federated systems. JSON is used similarly to XML, as a text-based data exchange format that typically uses attribute-value pairings, but it's not used for authentication and authorization exchange. HTML is used only for encoding web pages for web browsers and is not used for data exchange--and certainly not in a federated system.

NEW QUESTION: 352
A bare-metal hypervisor is Type _____.
A. 3
B. 4
C. 1
D. 2
Answer: C (LEAVE A REPLY)

NEW QUESTION: 353
Which of the following is a risk in the cloud environment that is not existing or is as prevalent in the legacy environment?
Response:
A. Ability of users to gain access to their physical workplace
B. Loss of productivity due to DDoS
C. Legal liability in multiple jurisdictions
D. Fire
Answer: C (LEAVE A REPLY)

NEW QUESTION: 354
What is the biggest negative to leasing space in a data center versus building or maintain your own?
A. Costs
B. Control
C. Certification
D. Regulation
Answer: B (LEAVE A REPLY)
When leasing space in a data center, an organization will give up a large degree of control as to how it is built and maintained, and instead must conform to the policies and procedures of the owners and operators of the data center.

NEW QUESTION: 355
Which of the following may unilaterally deem a cloud hosting model inappropriate for a system or application?
A. Multitenancy

B. Certification
C. Regulation
D. Virtualization
Answer: (SHOW ANSWER)
Explanation
Some regulations may require specific security controls or certifications be used for hosting certain types of data or functions, and in some circumstances they may be requirements that are unable to be met by any cloud provider.

NEW QUESTION: 356
Which of the following are cloud computing roles?
A. Cloud service broker and user
B. Cloud customer and financial auditor
C. CSP and backup service provider
D. Cloud service auditor and object
Answer: C (LEAVE A REPLY)
The following groups form the key roles and functions associated with cloud computing. They do not constitute an exhaustive list but highlight the main roles and functions within cloud computing:
- Cloud customer: An individual or entity that utilizes or subscribes to cloud based services or resources.
- CSP: A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations or individuals, usually for a fee; otherwise known to clients "as a service.
- Cloud backup service provider: A third-party entity that manages and holds operational responsibilities for cloud-based data backup services and solutions to customers from a central data center.
- CSB: Typically a third-party entity or company that looks to extend or enhance value to multiple customers of cloud-based services through relationships with multiple CSPs. It acts as a liaison between cloud services customers and CSPs, selecting the best provider for each customer and monitoring the services. The CSB can be utilized as a "middleman" to broker the best deal and customize services to the customer's requirements. May also resell cloud services.
- Cloud service auditor: Third-party organization that verifies attainment of SLAs.

NEW QUESTION: 357
Which of the following is NOT a core component of an SIEM solution?
Response:
A. Correlation
B. Escalation
C. Aggregation

D. Compliance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 358
The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program has _____ tiers.
Response:
A. Two
B. Three
C. Eight
D. Four
Answer: (SHOW ANSWER)

NEW QUESTION: 359
What controls the formatting and security settings of a volume storage system within a cloud environment?
A. Management plane
B. SAN host controller
C. Hypervisor
D. Operating system of the host
Answer: D (LEAVE A REPLY)
Once a storage LUN is allocated to a virtual machine, the operating system of that virtual machine will format, manage, and control the file system and security of the data on that LUN.

NEW QUESTION: 360
APIs are defined as which of the following?
A. A set of protocols, and tools for building software applications to access a web-based software application or tool
B. A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or tool
C. A set of standards for building software applications to access a web-based software application or tool
D. A set of routines and tools for building software applications to access web-based software applications
Answer: B (LEAVE A REPLY)
Explanation
All the answers are true, but B is the most complete.

NEW QUESTION: 361

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: 362

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)

Explanation

We don't use DAM in place of encryption or masking; DAM augments these options without replacing them.

We don't usually think of the database interaction as client-server, so A is the best answer.

NEW QUESTION: 363

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

A. The users of the various organizations within the federations within the federation/a CASB

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

NEW QUESTION: 364
Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company's website)?
A. SOC 3
B. SOC 1
C. SOC 2, Type 2
D. SOC 2, Type 1
Answer: (SHOW ANSWER)

NEW QUESTION: 365
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: 366
Which of the following methods of addressing risk is most associated with insurance?
Response:
A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

Answer: A (LEAVE A REPLY)

NEW QUESTION: 367
Which of the following tasks within a SaaS environment would NOT be something the cloud customer would be responsible for?
A. Authentication mechanism
B. Branding
C. Training
D. User access
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The authentication mechanisms and implementations are the responsibility of the cloud provider because they are core components of the application platform and service. Within a SaaS implementation, the cloud customer will provision user access, deploy branding to the application interface (typically), and provide or procure training for its users.

NEW QUESTION: 368
You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center.
One of the challenges you're facing is whether the provider will have undue control over your data once it is within the provider's data center; will the provider be able to hold your organization hostage because they have your data?
This is a(n) _____ issue.
Response:
A. Security
B. Interoperability
C. Availability
D. Portability
Answer: D (LEAVE A REPLY)

NEW QUESTION: 369
Which of the following contract terms most incentivizes the cloud provider to meet the requirements listed in the SLA?
A. Financial penalties
B. Performance details
C. Desire to maintain customer satisfaction
D. Regulatory oversight
Answer: A (LEAVE A REPLY)

NEW QUESTION: 370

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

NEW QUESTION: 371
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: 372
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. Private
B. Public
C. Community
D. Hybrid
Answer: A (LEAVE A REPLY)

NEW QUESTION: 373
Which of the following would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?
A. Resource pooling
B. Virtualization
C. Multitenancy
D. Regulation
Answer: (SHOW ANSWER)
Explanation/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: 374
Cloud environments pose many unique challenges for a data custodian to properly adhere to policies and the use of data. What poses the biggest challenge for a data custodian with a PaaS implementation, over and above the same concerns with IaaS?
A. Knowledge of systems
B. Contractual requirements
C. Access to systems
D. Data classification rules
Answer: A (LEAVE A REPLY)

NEW QUESTION: 375
Which of the following is the best example of a key component of regulated PII?
Response:
A. Items that should be implemented
B. Audit rights of subcontractors
C. Mandatory breach reporting
D. PCI DSS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 376
Log data should be protected _____.
Response:
A. One level below the sensitivity level of the systems from which it was collected
B. With encryption in transit, at rest, and in use
C. According to NIST guidelines
D. At least at the same sensitivity level as the systems from which it was collected
Answer: D (LEAVE A REPLY)

NEW QUESTION: 377
The BIA can be used to provide information about all the following, except:
Response:
A. BC/DR planning
B. Secure acquisition
C. Selection of security controls
D. Risk analysis
Answer: B (LEAVE A REPLY)

NEW QUESTION: 378
Data masking can be used to provide all of the following functionality, except:
A. Test data in sandboxed environments
B. Authentication of privileged users
C. Enforcing least privilege
D. Secure remote access
Answer: B (LEAVE A REPLY)
Explanation
Data masking does not support authentication in any way. All the others are excellent use cases for data masking.

NEW QUESTION: 379
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: 380
Which of the following roles is responsible for peering with other cloud services and providers?
A. Cloud auditor
B. Inter-cloud provider
C. Cloud service broker
D. Cloud service developer
Answer: B (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.

NEW QUESTION: 381
With finite resources available within a cloud, even the largest cloud providers will at times need to determine which customers will receive additional resources first.
What is the term associated with this determination?
A. Weighting
B. Prioritization
C. Shares
D. Scoring
Answer: C (LEAVE A REPLY)
Explanation
Shares are used within a cloud environment to prioritize resource allocation when customer requests exceed the available resources. Cloud providers utilize shares by assigning a priority score to each customer and allocating resources to those with the highest scores first. Scoring is a component of shares that determines the actual order in which to allocate resources. Neither weighting nor prioritization is the correct term in this case.

NEW QUESTION: 382
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.
Which of the following benefits will the CSA CCM offer your organization?
Response:
A. Simplifying regulatory compliance
B. Enforcing contract terms between your organization and the cloud provider
C. Ensuring that the baseline configuration is applied to all systems
D. Collecting multiple data streams from your log files
Answer: (SHOW ANSWER)

NEW QUESTION: 383
Which of the following service capabilities gives the cloud customer the most control over resources and configurations?
A. Desktop
B. Platform
C. Infrastructure
D. Software
Answer: C (LEAVE A REPLY)
The infrastructure service capability gives the cloud customer substantial control in provisioning and configuring resources, including processing, storage, and network resources.

NEW QUESTION: 384
What is a cloud storage architecture that manages the data in a hierarchy of files?
A. CDN
B. Database
C. Object-based storage
D. File-based storage
Answer: (SHOW ANSWER)

NEW QUESTION: 385
Because of multitenancy, specific risks in the public cloud that don't exist in the other cloud service models include all the following except:
A. DoS/DDoS
B. Information bleed
C. Risk of loss/disclosure due to legal seizures
D. Escalation of privilege
Answer: A (LEAVE A REPLY)
Explanation
DoS/DDoS threats and risks are not unique to the public cloud model.

NEW QUESTION: 386
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: 387
A localized incident or disaster can be addressed in a cost-effective manner by using which of the following?
A. UPS
B. Generators
C. Joint operating agreements
D. Strict adherence to applicable regulations
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Joint operating agreements can provide nearby relocation sites so that a disruption limited to the organization's own facility and campus can be addressed at a different facility and campus. UPS and generators are not limited to serving needs for localized causes. Regulations do not promote cost savings and are not often the immediate concern during BC/DR activities.

NEW QUESTION: 388
What is the intellectual property protection for a useful manufacturing innovation?
A. Trademark
B. Copyright
C. patent
D. Trade secret
Answer: (SHOW ANSWER)
Patents protect processes (as well as inventions, new plantlife, and decorative patterns). The other answers listed are answers to other questions.

NEW QUESTION: 389
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)
Explanation

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

NEW QUESTION: 390
Which of the following actions will NOT make data part of the "create" phase of the cloud data lifecycle?
A. Modifying metadata
B. Importing data
C. Modifying data
D. Constructing new data
Answer: A (LEAVE A REPLY)
Although the 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 modified into a new form or value. Modifying the metadata does not change the actual data.

NEW QUESTION: 391
The cloud deployment model that features joint ownership of assets among an affinity group is known as:
Response:
A. Private
B. Public
C. Hybrid
D. Community
Answer: D (LEAVE A REPLY)

NEW QUESTION: 392
Which of the following is the biggest concern or challenge with using encryption?
A. Dependence on keys
B. Cipher strength

C. Efficiency
D. Protocol standards
Answer: (SHOW ANSWER)
Explanation
No matter what kind of application, system, or hosting model used, encryption is 100 percent dependent on encryption keys. Properly securing the keys and the exchange of them is the biggest and most important challenge of encryption systems.

NEW QUESTION: 393
Digital investigations have adopted many of the same methodologies and protocols as other types of criminal or scientific inquiries.
What term pertains to the application of scientific norms and protocols to digital investigations?
A. Scientific
B. Investigative
C. Methodological
D. Forensics
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Forensics refers to the application of scientific methods and protocols to the investigation of crimes.
Although forensics has traditionally been applied to well-known criminal proceedings and investigations, the term equally applies to digital investigations and methods. Although the other answers provide similar- sounding terms and ideas, none is the appropriate answer in this case.

NEW QUESTION: 394
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: 395
Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:
A. The cloud provider's suppliers
B. The cloud provider's vendors
C. The cloud provider's utilities
D. The cloud provider's resellers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 396
Different types of audits are intended for different audiences, such as internal, external, regulatory, and so on.
Which of the following audits are considered "restricted use" versus being for a more broad audience?
A. SOC Type 2
B. SOC Type 1
C. SOC Type 3
D. SAS-70
Answer: (SHOW ANSWER)

Explanation
SOC Type 1 reports are intended for restricted use, only to be seen by the actual service organization, its current clients, or its auditors. These reports are not intended for wider or public distribution.SAS-70 audit reports have been deprecated and are no longer in use, and both the SOC Type 2 and 3 reports are designed to expand upon the SOC Type 1 reports and are for broader audiences.

NEW QUESTION: 397
When a data center is configured such that the backs of the devices face each other and the ambient temperature in the work area is cool, it is called _____.
A. HVAC modulated
B. Cold aisle containment
C. Hot aisle containment
D. Thermo-optimized
Answer: C (LEAVE A REPLY)

NEW QUESTION: 398
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: B (LEAVE A REPLY)
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: 399
In a cloud environment, encryption should be used for all the following, except:
A. Secure sessions/VPN
B. Long-term storage of data
C. Near-term storage of virtualized images
D. Profile formatting
Answer: (SHOW ANSWER)
All of these activities should incorporate encryption, except for profile formatting, which is a made-up term.

NEW QUESTION: 400
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: 401
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:
IPSec is a protocol for encrypting and authenticating packets during transmission between two parties and can involve any type of device, application, or service. The protocol performs both the authentication and negotiation of security policies between the two parties at the start of the connection and then maintains these policies throughout the lifetime of the connection. TLS operates at the application layer, not the network layer, and is widely used to secure communications between two parties. SSL is similar to TLS but has been deprecated. Although a VPN allows a secure channel for communications into a private network from an outside location, it's not a protocol.

NEW QUESTION: 402
Which of the following service capabilities gives the cloud customer an established and maintained framework to deploy code and applications?
A. Software
B. Desktop
C. Platform
D. Infrastructure
Answer: C (LEAVE A REPLY)
Explanation
The platform service capability provides programming languages and libraries from the cloud provider, where the customer can deploy their own code and applications into a managed and controlled framework.

NEW QUESTION: 403
Which aspect of cloud computing serves as the biggest challenge to using DLP to protect data at rest?
A. Portability
B. Resource pooling
C. Interoperability
D. Reversibility
Answer: B (LEAVE A REPLY)
Resource pooling serves as the biggest challenge to using DLP solutions to protect data at rest because data is spread across large systems, which are also shared by many different clients. With the data always moving and being distributed, additional challenges for protection are created versus a physical and isolated storage system. Portability is the ability to easily move between different cloud providers, and interoperability is focused on the ability to reuse components or services. Reversibility pertains to the ability of a cloud customer to easily and completely remove their data and services from a cloud provider.

NEW QUESTION: 404
Which of the following is a method for apportioning resources that involves prioritizing resource requests to resolve contention situations?
A. Cancellations
B. Shares
C. Reservations
D. Limits
Answer: B (LEAVE A REPLY)

NEW QUESTION: 405
The baseline should cover which of the following?
A. Data breach alerting and reporting
B. All regulatory compliance requirements
C. As many systems throughout the organization as possible
D. A process for version control
Answer: C (LEAVE A REPLY)
Explanation
The more systems that be included in the baseline, the more cost-effective and scalable the baseline is. The baseline does not deal with breaches or version control; those are the provinces of the security office and CMB, respectively. Regulatory compliance might (and usually will) go beyond the baseline and involve systems, processes, and personnel that are not subject to the baseline.

NEW QUESTION: 406

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

A. Segregated from host systems

B. Network access

C. Scalability

D. External to system patching

Answer: (SHOW ANSWER)

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

Network access is not a consideration because both a host-based IDS and a network-based IDS would have access to network resources.

NEW QUESTION: 407

Which of the following is NOT an application or utility to apply and enforce baselines on a system?

A. Chef

B. GitHub

C. Puppet

D. Active Directory

Answer: B (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 408

What strategy involves hiding data in a data set to prevent someone from identifying specific individuals based on other data fields present?

A. Anonymization

B. Tokenization

C. Masking

D. Obfuscation

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

With data anonymization, data is manipulated in such a way so as to prevent the identification of an individual through various data objects, and is often used in conjunction with other concepts such as masking.

NEW QUESTION: 409

Which of the following represents a minimum guaranteed resource within a cloud environment for the cloud customer?

A. Reservation

B. Share

C. Limit

D. Provision

Answer: A (LEAVE A REPLY)

A reservation is a minimum resource that is guaranteed to a customer within a cloud environment. Within a cloud, a reservation can pertain to the two main aspects of computing: memory and processor. With a reservation in place, the cloud provider guarantees that a cloud customer will always have at minimum the necessary resources available to power on and operate any of their services.

NEW QUESTION: 410

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

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

B. Refrain from storing credentials long term.

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

D. Implement digital rights management (DRM) solutions.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 411
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)
Explanation
Business continuity and disaster recovery (BCDR) solutions largely sit idle until they are actually needed. This traditionally has led to increased costs for an organization because physical hardware must be purchased and operational but is not used. By using a cloud system, an organization will only pay for systems when they are being used and only for the duration of use, thus eliminating the need for extra hardware and costs. Portability is the ability to easily move services among different cloud providers. Broad network access allows access to users and staff from anywhere and from different clients, and although this would be important for a BCDR situation, it is not the best answer in this case. On-demand self-service allows users to provision services automatically and when needed, and although this too would be important for BCDR situations, it is not the best answer because it does not address costs or the biggest benefits to an organization.

NEW QUESTION: 412
What concept does the "I" represent with the STRIDE threat model?
A. Integrity
B. Information disclosure
C. IT security
D. Insider threat
Answer: (SHOW ANSWER)
Explanation
Perhaps the biggest concern for any user is having their personal and sensitive information disclosed by an application. There are many aspects of an application to consider with security and protecting this information, and it is very difficult for any application to fully ensure security from start to finish. The obvious focus is on security within the application itself, as well as protecting and storing the data.

NEW QUESTION: 413
Which is the appropriate phase of the cloud data lifecycle for determining the data's classification?
A. Create
B. Use
C. Share

D. Store
Answer: (SHOW ANSWER)
Explanation
Explanation:
Any time data is created, modified, or imported, the classification needs to be evaluated and set from the earliest phase to ensure security is always properly maintained for the duration of its lifecycle.

NEW QUESTION: 414
Which of the following is not a component of the of the STRIDE model?
Response:
A. External pen testing
B. Information disclosure
C. Spoofing
D. Repudiation
Answer: (SHOW ANSWER)

NEW QUESTION: 415
Which of the following is NOT a criterion for data within the scope of eDiscovery?
A. Possession
B. Custody
C. Control
D. Archive
Answer: D (LEAVE A REPLY)
Explanation
eDiscovery pertains to information and data that is in the possession, control, and custody of an organization.

NEW QUESTION: 416
How is an object stored within an object storage system?
A. Key value
B. Database
C. LDAP
D. Tree structure
Answer: A (LEAVE A REPLY)
Explanation
Object storage uses a flat structure with key values to store and access objects.

NEW QUESTION: 417
What is the experimental technology that might lead to the possibility of processing encrypted data without having to decrypt it first?

A. One-time pads
B. Link encryption
C. Homomorphic encryption
D. AES
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
AES is an encryption standard. Link encryption is a method for protecting communications traffic. One-time pads are an encryption method.

NEW QUESTION: 418
When is a virtual machine susceptible to attacks while a physical server in the same state would not be?
A. When it is behind a WAF
B. When it is behind an IPS
C. When it is not patched
D. When it is powered off
Answer: D (LEAVE A REPLY)
A virtual machine is ultimately an image file residing a file system. Because of this, even when a virtual machine is "powered off," it is still susceptible to attacks and modification. A physical server that is powered off would not be susceptible to attacks.

NEW QUESTION: 419
Which format is the most commonly used standard for exchanging information within a federated identity system?
A. XML
B. HTML
C. SAML
D. JSON
Answer: C (LEAVE A REPLY)
Security Assertion Markup Language (SAML) is the most common data format for information exchange within a federated identity system. It is used to transmit and exchange authentication and authorization data.XML is similar to SAML, but it's used for general-purpose data encoding and labeling and is not used for the exchange of authentication and authorization data in the way that SAML is for federated systems. JSON is used similarly to XML, as a text-based data exchange format that typically uses attribute- value pairings, but it's not used for authentication and authorization exchange. HTML is used only for encoding web pages for web browsers and is not used for data exchange--and certainly not in a federated system.

NEW QUESTION: 420

Which networking concept in a cloud environment allows for network segregation and isolation of IP spaces?

A. PLAN

B. WAN

C. LAN

D. VLAN

Answer: D (LEAVE A REPLY)

A virtual area network (VLAN) allows the logical separation and isolation of networks and IP spaces to provide enhanced security and controls.

NEW QUESTION: 421

What concept and operational process must be spelled out clearly, as far as roles and responsibilities go, between the cloud provider and cloud customer for the mitigation of any problems or security events?

A. Incident response

B. Problem management

C. Change management

D. Conflict response

Answer: A (LEAVE A REPLY)

Explanation

Incident response is the process through which security or operational issues are handled, including and coordination with and communication to the appropriate stakeholders. None of the other terms provided is the correct response.

NEW QUESTION: 422

All the following are data analytics modes, except:

A. Datamining

B. Agile business intelligence

C. Refractory iterations

D. Real-time analytics

Answer: (SHOW ANSWER)

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

NEW QUESTION: 423
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/Reference:
Explanation:
DNSSEC is designed to prevent the spoofing and redirection of DNS resolutions to rogue sites.

NEW QUESTION: 424
Federation should be _____ to the users.
Response:
A. Proportional
B. Hostile
C. Expensive
D. Transparent
Answer: (SHOW ANSWER)

NEW QUESTION: 425
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the amount of data and services needed to reach the predetermined level of operations?
A. SRE
B. RPO
C. RSL
D. RTO
Answer: B (LEAVE A REPLY)
The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the predetermined level of operations necessary during a BCDR situation.
The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. SRE is provided as an erroneous response.

NEW QUESTION: 426
Which of the following is NOT a major regulatory framework?
A. PCI DSS
B. HIPAA
C. SOX
D. FIPS 140-2
Answer: D (LEAVE A REPLY)
Explanation
Explanation:
FIPS 140-2 is a United States certification standard for cryptographic modules, and it provides guidance and requirements for their use based on the requirements of the data classification. However, these are not actual regulatory requirements. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS) are all major regulatory frameworks either by law or specific to an industry.

NEW QUESTION: 427
Which of the following report is most aligned with financial control audits?
A. SSAE 16
B. SOC 2
C. SOC 1
D. SOC 3
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The SOC 1 report focuses primarily on controls associated with financial services. While IT controls are certainly part of most accounting systems today, the focus is on the controls around those financial systems.

NEW QUESTION: 428
A honeypot should contain _____ data.
A. Production
B. Sensitive
C. Raw
D. Useless
Answer: (SHOW ANSWER)

NEW QUESTION: 429
What is a key capability or characteristic of PaaS?
A. Support for a homogenous environment

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

NEW QUESTION: 430
Which of the following frameworks focuses specifically on design implementation and management?
A. ISO 31000:2009
B. ISO 27017
C. NIST 800-92
D. HIPAA

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

NEW QUESTION: 431
Resolving resource contentions in the cloud will most likely be the job of the _____.
Response:
A. Regulator
B. Router
C. Emulator
D. Hypervisor
Answer: D (LEAVE A REPLY)

NEW QUESTION: 432
An audit against the _____ will demonstrate that an organization has a holistic, comprehensive security program.
Response:
A. SSAE 16 standard
B. SOC 2, Type 2 report matrix
C. ISO 27001 certification requirements
D. SAS 70 standard
Answer: C (LEAVE A REPLY)

NEW QUESTION: 433
It is important to include _____ in the design of underfloor plenums if they are also used for wiring.
Response:
A. Sequestered channels
B. Tight gaskets
C. Mantraps
D. Heat sinks
Answer: B (LEAVE A REPLY)

NEW QUESTION: 434
What's a potential problem when object storage versus volume storage is used within IaaS for application use and dependency?
A. Object storage is only optimized for small files.
B. Object storage is its own system, and data consistency depends on replication.
C. Object storage may have availability issues.

D. Object storage is dependent on access control from the host server.

Answer: B (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 435

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: 436

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)

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: 437
Which of the following publishes the most commonly used standard for data center design in regard to tiers and topologies?
A. IDCA
B. Uptime Institute
C. NFPA
D. BICSI
Answer: B (LEAVE A REPLY)
The Uptime Institute publishes the most commonly used and widely known standard on data center tiers and topologies. It is based on a series of four tiers, with each progressive increase in number representing more stringent, reliable, and redundant systems for security, connectivity, fault tolerance, redundancy, and cooling.

NEW QUESTION: 438
The tasks performed by the hypervisor in the virtual environment can most be likened to the tasks of the
_____ in the legacy environment.
Response:
A. Central processing unit (CPU)
B. OS
C. Security team
D. PGP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 439

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

NEW QUESTION: 440
What type of masking strategy involves making a separate and distinct copy of data with masking in place?
A. Dynamic
B. Replication
C. Static
D. Duplication
Answer: C (LEAVE A REPLY)
With static masking, a separate and distinct copy of the data set is created with masking in place. This is typically done through a script or other process that takes a standard data set, processes it to mask the appropriate and predefined fields, and then outputs the data set as a new one with the completed masking done.

NEW QUESTION: 441
There are many situations when testing a BCDR plan is appropriate or mandated.
Which of the following would not be a necessary time to test a BCDR plan?
A. After software updates
B. After regulatory changes
C. After major configuration changes
D. Annually
Answer: B (LEAVE A REPLY)
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: 442
A localized incident or disaster can be addressed in a cost-effective manner by using which of the following?
A. UPS
B. Generators
C. Joint operating agreements
D. Strict adherence to applicable regulations
Answer: (SHOW ANSWER)
Explanation
Joint operating agreements can provide nearby relocation sites so that a disruption limited to the organization's own facility and campus can be addressed at a different facility and campus. UPS and generators are not limited to serving needs for localized causes. Regulations do not promote cost savings and are not often the immediate concern during BC/DR activities.

NEW QUESTION: 443
Before deploying a specific brand of virtualization toolset, it is important to configure it according to _____.
A. Expert opinion
B. Industry standards
C. Vendor guidance
D. Prevailing law of that jurisdiction
Answer: C (LEAVE A REPLY)

NEW QUESTION: 444
In order to prevent cloud customers from potentially consuming enormous amounts of resources within a cloud environment and thus having a negative impact on other customers, what concept is commonly used by a cloud provider?
A. Limit
B. Cap
C. Throttle
D. Reservation
Answer: A (LEAVE A REPLY)
A limit puts a maximum value on the amount of resources that may be consumed by either a system, a service, or a cloud customer. It is commonly used to prevent one entity from consuming enormous amounts of resources and having an operational impact on other tenants within the same cloud system. Limits can either be hard or somewhat flexible, meaning a customer can borrow from other customers while still having their actual limit preserved. A reservation is a guarantee to a cloud customer that a certain level of resources will always be available to them, regardless of what operational demands are

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

NEW QUESTION: 445
DNSSEC was designed to add a layer of security to the DNS protocol.
Which type of attack was the DNSSEC extension designed to mitigate?
A. Account hijacking
B. Snooping
C. Spoofing
D. Data exposure
Answer: (SHOW ANSWER)
DNSSEC is an extension to the regular DNS protocol that utilizes digital signing of DNS query results, which can be verified to come from an authoritative source. This verification mitigates the ability for a rogue DNS server to be used to spoof query results and to direct users to malicious sites. DNSSEC provides for the verification of the integrity of DNS queries. It does not provide any protection from snooping or data exposure.
Although it may help lessen account hijacking by preventing users from being directed to rogue sites, it cannot by itself eliminate the possibility.

NEW QUESTION: 446
The cloud deployment model that features organizational ownership of the hardware and infrastructure, and usage only by members of that organization, is known as:
A. Motive
B. Public
C. Private
D. Hybrid
Answer: (SHOW ANSWER)

NEW QUESTION: 447
One of the main components of system audits is the ability to track changes over time and to match these changes with continued compliance and internal processes.
Which aspect of cloud computing makes this particular component more challenging than in a traditional data center?
A. Portability
B. Virtualization
C. Elasticity
D. Resource pooling
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:

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

NEW QUESTION: 448
Which of the following is NOT a component of access control?
A. Accounting
B. Federation
C. Authorization
D. Authentication
Answer: B (LEAVE A REPLY)
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: 449
Although much of the attention given to data security is focused on keeping data private and only accessible by authorized individuals, of equal importance is the trustworthiness of the data.
Which concept encapsulates this?
A. Validity
B. Integrity
C. Accessibility
D. Confidentiality
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Integrity refers to the trustworthiness of data and whether its format and values are true and have not been corrupted or otherwise altered through unauthorized means.

Confidentiality refers to keeping data from being access or viewed by unauthorized parties. Accessibility means that data is available and ready when needed by a user or service. Validity can mean a variety of things that are somewhat similar to integrity, but it's not the most appropriate answer in this case.

NEW QUESTION: 450
Which of the following is not a component of contractual PII?
A. Scope of processing
B. Value of data
C. Location of data
D. Use of subcontractors
Answer: C (LEAVE A REPLY)
Explanation
The value of data itself has nothing to do with it being considered a part of contractual

NEW QUESTION: 451
Which of the following methods for the safe disposal of electronic records can always be used in a cloud environment?
Response:
A. Physical destruction
B. Degaussing
C. Encryption
D. Overwriting
Answer: (SHOW ANSWER)

NEW QUESTION: 452
Which of the following is NOT a common component of a DLP implementation process?
Response:
A. Discovery
B. Monitoring
C. Revision
D. Enforcement

Answer: (SHOW ANSWER)

NEW QUESTION: 453
Which standards body depends heavily on contributions and input from its open membership base?
A. CSA
B. ICANN
C. ISO
D. NIST
Answer: A (LEAVE A REPLY)

NEW QUESTION: 454
Security is a critical yet often overlooked consideration for BCDR planning.
At which stage of the planning process should security be involved?
A. Scope definition
B. Requirements gathering
C. Analysis
D. Risk assessment
Answer: (SHOW ANSWER)
Defining the scope of the plan is the very first step in the overall process. Security should be included from the very earliest stages and throughout the entire process. Bringing in security at a later stage can lead to additional costs and time delays to compensate for gaps in planning. Risk assessment, requirements gathering, and analysis are all later steps in the process, and adding in security at any of those points can potentially cause increased costs and time delays.

NEW QUESTION: 455
Where is an XML firewall most commonly deployed in the environment?
A. Between the application and data layers
B. Between the IPS and firewall
C. Between the presentation and application layers
D. Between the firewall and application server
Answer: D (LEAVE A REPLY)
Explanation
XML firewalls are most commonly deployed in line between the firewall and application server to validate XML code before it reaches the application.

NEW QUESTION: 456
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/Reference:
Explanation:
All the answers are true, but B is the most complete.

NEW QUESTION: 457
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: 458
Which cloud service category would be most ideal for a cloud customer that is developing software to test its applications among multiple hosting providers to determine the best option for its needs?
A. DaaS
B. PaaS
C. IaaS
D. SaaS
Answer: B (LEAVE A REPLY)
Platform as a Service would allow software developers to quickly and easily deploy their applications among different hosting providers for testing and validation in order to determine the best option. Although IaaS would also be appropriate for hosting

applications, it would require too much configuration of application servers and libraries in order to test code. Conversely, PaaS would provide a ready-to-use environment from the onset. DaaS would not be appropriate in any way for software developers to use to deploy applications. IaaS would not be appropriate in this scenario because it would require the developers to also deploy and maintain the operating system images or to contract with another firm to do so. SaaS, being a fully functional software platform, would not be appropriate for deploying applications into.

NEW QUESTION: 459
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/Reference:
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: 460
Which of the following jurisdictions lacks a comprehensive national policy on data privacy and the protection of personally identifiable information (PII)?
A. European Union
B. Asian-Pacific Economic Cooperation
C. United States
D. Russia
Answer: (SHOW ANSWER)
The United States has a myriad of regulations focused on specific types of data, such as healthcare and financial, but lacks an overall comprehensive privacy law on the national level.
The European Union, the Asian-Pacific Economic Cooperation, and Russia all have national privacy protections and regulations for the handling the PII data of their citizens.

NEW QUESTION: 461

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

NEW QUESTION: 462
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: (SHOW ANSWER)
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: 463
Which component of ITIL involves the creation of an RFC ticket and obtaining official approvals for it?
A. Problem management
B. Release management
C. Deployment management
D. Change management
Answer: (SHOW ANSWER)
The change management process involves the creation of the official Request for Change (RFC) ticket, which is used to document the change, obtain the required approvals from management and stakeholders, and track the change to completion. Release management is a subcomponent of change management, where the actual code or configuration change is put into place. Deployment management is similar to release management, but it's where changes are actually implemented on systems. Problem management is focused on the identification and mitigation of known problems and deficiencies before they are able to occur.

NEW QUESTION: 464
A process for _____ can aid in protecting against data disclosure due to lost devices.

A. Device tracking
B. Credential revocation
C. User punishment
D. Law enforcement notification
Answer: (SHOW ANSWER)

NEW QUESTION: 465
With a cloud service category where the cloud customer is responsible for deploying all services, systems, and components needed for their applications, which of the following storage types are MOST likely to be available to them?
A. Structured and hierarchical
B. Volume and object
C. Volume and database
D. Structured and unstructured
Answer: (SHOW ANSWER)
The question is describing the Infrastructure as a Service (IaaS) cloud offering, and as such, the volume and object storage types will be available to the customer. Structured and unstructured are storage types associated with PaaS, and although the other answers present similar- sounding storage types, they are a mix of real and fake names.

NEW QUESTION: 466
Which of the following are not examples of personnel controls?
Response:
A. Continuous security training
B. Strict access control mechanisms
C. Background checks
D. Reference checks
Answer: B (LEAVE A REPLY)

NEW QUESTION: 467
Which phase of the cloud data lifecycle also typically entails the process of data classification?

A. Use
B. Create
C. Archive
D. Store
Answer: B (LEAVE A REPLY)

NEW QUESTION: 468
The president of your company has tasked you with implementing cloud services as the most efficient way of obtaining a robust disaster recovery configuration for your production services.
Which of the cloud deployment models would you MOST likely be exploring?
A. Hybrid
B. Private
C. Community
D. Public
Answer: (SHOW ANSWER)
A hybrid cloud model spans two more different hosting configurations or cloud providers. This would enable an organization to continue using its current hosting configuration, while adding additional cloud services to enable disaster recovery capabilities. The other cloud deployment models--public, private, and community--would not be applicable for seeking a disaster recovery configuration where cloud services are to be leveraged for that purpose rather than production service hosting.

NEW QUESTION: 469
Which phase of the cloud data lifecycle involves processing by a user or application?
Response:
A. Create
B. Share
C. Store
D. Use
Answer: (SHOW ANSWER)

NEW QUESTION: 470
Countermeasures for protecting cloud operations against internal threats include all of the following except:
A. Extensive and comprehensive training programs, including initial, recurring, and refresher sessions
B. Skills and knowledge testing
C. Hardened perimeter devices
D. Aggressive background checks
Answer: (SHOW ANSWER)

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

NEW QUESTION: 471
Which type of cloud-based storage is IRM typically associated with?
Response:
A. Structured
B. Volume
C. Object
D. Unstructured
Answer: (SHOW ANSWER)

NEW QUESTION: 472
Which of the following threat types involves an application that does not validate authorization for portions of itself after the initial checks?
A. Injection
B. Missing function-level access control
C. Cross-site request forgery
D. Cross-site scripting
Answer: B (LEAVE A REPLY)
Explanation
It is imperative that an application perform checks when each function or portion of the application is accessed, to ensure that the user is properly authorized to access it. Without continual checks each time a function is accessed, an attacker could forge requests to access portions of the application where authorization has not been granted.

NEW QUESTION: 473
What is the federal agency that accepts applications for new patents?
A. USPTO
B. SEC
C. OSHA
D. USDA
Answer: (SHOW ANSWER)

NEW QUESTION: 474
Which aspect of SaaS will alleviate much of the time and energy organizations spend on compliance (specifically baselines)?
A. Maintenance
B. Licensing
C. Standardization
D. Development
Answer: (SHOW ANSWER)

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

NEW QUESTION: 475
Which of the following is NOT a focus or consideration of an internal audit?
A. Certification
B. Design
C. Costs
D. Operational efficiency
Answer: A (LEAVE A REPLY)
In order to obtain and comply with certifications, independent external audits must be performed and satisfied. Although some testing of certification controls can be part of an internal audit, they will not satisfy requirements.

NEW QUESTION: 476
What does the REST API support that SOAP does NOT support?
A. Caching
B. Encryption
C. Acceleration
D. Redundancy
Answer: A (LEAVE A REPLY)
The SOAP protocol does not support caching, whereas the REST API does.

NEW QUESTION: 477
What is a cloud storage architecture that manages the data in caches of copied content close to locations of high demand?
Response:
A. Database
B. CDN
C. Object-based storage
D. File-based storage
Answer: (SHOW ANSWER)

NEW QUESTION: 478
When using a PaaS solution, what is the capability provided to the customer?

A. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the provider supports. The provider does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
B. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the provider supports. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
C. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the consumer supports. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
D. To deploy onto the cloud infrastructure provider-created or acquired applications created using programming languages, libraries, services, and tools that the provider supports. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Answer: (SHOW ANSWER)
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: 479
All of the following are identity federation standards commonly found in use today except _____.
Response:
A. OAuth
B. OpenID
C. WS-Federation
D. PGP

Answer: D (LEAVE A REPLY)

NEW QUESTION: 480
Penetration testing is a(n) _____ form of security assessment.
A. Inexpensive
B. Total
C. Comprehensive
D. Active
Answer: D (LEAVE A REPLY)

NEW QUESTION: 481
Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?
A. Regulation
B. Multitenancy
C. Virtualization
D. Resource pooling
Answer: B (LEAVE A REPLY)
With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers. Especially within a public cloud model, it is not possible or practical for a cloud provider to alter its services for specific customer demands.
Resource pooling and virtualization within a cloud environment would be the same for all customers, and would not impact certifications that a cloud provider might be willing to pursue.
Regulations would form the basis for certification problems and would be a reason for a cloud provider to pursue specific certifications to meet customer requirements.

NEW QUESTION: 482
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: 483

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

A. Record

B. Binding

C. Negotiation

D. Handshake

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 484

Which of the following would NOT be a reason to activate a BCDR strategy?

A. Staffing loss

B. Terrorism attack

C. Utility disruptions

D. Natural disaster

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:
The loss of staffing would not be a reason to declare a BCDR situation because it does not impact production operations or equipment, and the same staff would be needed for a BCDR situation.

NEW QUESTION: 485
What is a standard configuration and policy set that is applied to systems and virtual machines called?
A. Standardization
B. Baseline
C. Hardening
D. Redline
Answer: B (LEAVE A REPLY)
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: 486
What concept does the "R" represent with the DREAD model?
A. Reproducibility
B. Repudiation
C. Risk
D. Residual
Answer: A (LEAVE A REPLY)
Reproducibility is the measure of how easy it is to reproduce and successful use an exploit. Scoring within the DREAD model ranges from 0, signifying a nearly impossibly exploit, up to 10, which signifies something that anyone from a simple function call could exploit, such as a URL.

NEW QUESTION: 487
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:
A. Masking
B. Obfuscation
C. Tokenization
D. Data discovery
Answer: D (LEAVE A REPLY)

NEW QUESTION: 488
All the following are data analytics modes, except:
A. Datamining
B. Agile business intelligence
C. Refractory iterations
D. Real-time analytics
Answer: (SHOW ANSWER)
Explanation
All the others are data analytics methods, but "refractory iterations" is a nonsense term thrown in as a red herring.

NEW QUESTION: 489
You work for a government research facility. Your organization often shares data with other government research organizations.
You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations.
Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.
If you don't use cross-certification, what other model can you implement for this purpose?
Response:
A. Third-party identity broker
B. Mandatory access control (MAC)
C. Cloud reseller
D. Intractable nuanced variance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 490
Clustered systems can be used to ensure high availability and load balancing across individual systems through a variety of methodologies.
What process is used within a clustered system to ensure proper load balancing and to maintain the health of the overall system to provide high availability?
A. Distributed clustering
B. Distributed balancing
C. Distributed optimization
D. Distributed resource scheduling
Answer: (SHOW ANSWER)
Distributed resource scheduling (DRS) is used within all clustered systems as the method for providing high availability, scaling, management, workload distribution, and the balancing of jobs and processes.

None of the other choices is the correct term in this case.

NEW QUESTION: 491
Which of the following is NOT a regulatory system from the United States federal government?
A. PCI DSS
B. FISMA
C. SOX
D. HIPAA
Answer: (SHOW ANSWER)
Explanation
The payment card industry data security standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry regulatory standard, not a governmental one.

NEW QUESTION: 492
Many of the traditional concepts of systems and services for a traditional data center also apply to the cloud.
Both are built around key computing concepts.
Which of the following compromise the two facets of computing?
A. CPU and software
B. CPU and storage
C. CPU and memory
D. Memory and networking
Answer: C (LEAVE A REPLY)
The CPU and memory resources of an environment together comprise its "computing" resources. Cloud environments, especially public clouds, are enormous pools of resources for computing and are typically divided among a large number of customers with constantly changing needs and demands. Although storage and networking are core components of a cloud environment, they do not comprise its computing core.
Software, much like within a traditional data center, is highly subjective based on the application, system, service, or cloud computing model used; however, it is not one of the core cloud components.

NEW QUESTION: 493
Which of the cloud cross-cutting aspects relates to the ability to reuse or move components of an application or service?
A. Availability
B. Interoperability
C. Reversibility
D. Portability

Answer: B (LEAVE A REPLY)
Explanation
Interoperability is the ease with which one can move or reuse components of an application or service. This is maximized when services are designed without specific dependencies on underlying platforms, operating systems, locations, or cloud providers.

NEW QUESTION: 494
When an API is being leveraged, it will encapsulate its data for transmission back to the requesting party or service.
What is the data encapsulation used with the SOAP protocol referred to as?
A. Packet
B. Payload
C. Object
D. Envelope
Answer: (SHOW ANSWER)
Explanation
Simple Object Access Protocol (SOAP) encapsulates its information in what is known as a SOAP envelope. It then leverages common communications protocols for transmission. Object is a type of cloud storage, but also a commonly used term with certain types of programming languages. Packet and payload are terms that sound similar to envelope but are not correct in this case.

NEW QUESTION: 495
Which is the lowest level of the CSA STAR program?
A. Attestation
B. Self-assessment
C. Hybridization
D. Continuous monitoring
Answer: B (LEAVE A REPLY)
Explanation
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: 496
Which of the following threat types can occur when baselines are not appropriately applied or when unauthorized changes are made?
A. Security misconfiguration
B. Insecure direct object references
C. Unvalidated redirects and forwards
D. Sensitive data exposure

Answer: (SHOW ANSWER)
Explanation/Reference:
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: 497
Before deploying a specific brand of virtualization toolset, it is important to configure it according to _____.
Response:
A. Expert opinion
B. Industry standards
C. Vendor guidance
D. Prevailing law of that jurisdiction
Answer: C (LEAVE A REPLY)

NEW QUESTION: 498
In order to comply with regulatory requirements, which of the following secure erasure methods would be available to a cloud customer using volume storage within the IaaS service model?
A. Demagnetizing
B. Shredding
C. Degaussing

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

NEW QUESTION: 499
Designers making applications for the cloud have to take into consideration risks and operational constraints that did not exist or were not as pronounced in the legacy environment.
Which of the following is an element cloud app designers may have to consider incorporating in software for the cloud that might not have been as important in the legacy environment?
Response:
A. DDoS resistance
B. IAM capability
C. Field validation
D. Encryption for data at rest and in motion
Answer: D (LEAVE A REPLY)

NEW QUESTION: 500
Which of the following would NOT be used to determine the classification of data?
Response:
A. Metadata
B. Future use
C. Creator
D. PII
Answer: B (LEAVE A REPLY)

NEW QUESTION: 501
Which of the following threat types involves leveraging a user's browser to send untrusted data to be executed with legitimate access via the user's valid credentials?
A. Injection
B. Missing function-level access control
C. Cross-site scripting
D. Cross-site request forgery
Answer: D (LEAVE A REPLY)
Explanation

ExplanationCross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or perhaps the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with their own access and permissions, allowing the attacker to redirect the user's web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.

NEW QUESTION: 502
Heating, ventilation, and air conditioning (HVAC) systems cool the data center by pushing warm air into _____.
Response:
A. The outside world
B. The server inlets
C. HVAC intakes
D. Underfloor plenums
Answer: (SHOW ANSWER)

NEW QUESTION: 503
Which aspect of archiving must be tested regularly for the duration of retention requirements?
A. Availability
B. Recoverability
C. Auditability
D. Portability
Answer: (SHOW ANSWER)
In order for any archiving system to be deemed useful and compliant, regular tests must be performed to ensure the data can still be recovered and accessible, should it ever be needed, for the duration of the retention requirements.

NEW QUESTION: 504
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)
Explanation
Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Configuration management tracks and maintains detailed information about all IT components within an organization.

NEW QUESTION: 505
During which phase of the cloud data lifecycle is it possible for the classification of data to change?
A. Use
B. Archive
C. Create
D. Share
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The create phase encompasses any time data is created, imported, or modified. With any change in the content or value of data, the classification may also change. It must be continually reevaluated to ensure proper security. During the use, share, and archive phases, the data is not modified in any way, so the original classification is still relevant.

NEW QUESTION: 506
In order to comply with regulatory requirements, which of the following secure erasure methods would be available to a cloud customer using volume storage within the IaaS service model?
A. Demagnetizing
B. Shredding
C. Degaussing
D. Cryptographic erasure
Answer: D (LEAVE A REPLY)
Cryptographic erasure is a secure method to destroy data by destroying the keys that were used to encrypt it. This method is universally available for volume storage on IaaS and is also extremely quick.
Shredding, degaussing, and demagnetizing are all physically destructive methods that would not be permitted within a cloud environment using shared resources.

NEW QUESTION: 507
You were recently hired as a project manager at a major university to implement cloud services for the academic and administrative systems. Because the load and demand for services at a university are very cyclical in nature, commensurate with the academic calendar, which of the following aspects of cloud computing would NOT be a primary benefit to you?
A. Measured service
B. Broad network access
C. Resource pooling
D. On-demand self-service
Answer: (SHOW ANSWER)
Explanation
Broad network access to cloud services, although it is an integral aspect of cloud computing, would not being a specific benefit to an organization with cyclical business needs. The other options would allow for lower costs during periods of low usage as well as provide the ability to expand services quickly and easily when needed for peak periods. Measured service allows a cloud customer to only use the resources it needs at the time, and resource pooling allows a cloud customer to access resources as needed. On-demand self-service enables the cloud customer to change its provisioned resources on its own, without the need to interact with the staff from the cloud provider.

NEW QUESTION: 508
Which of the following technologies is used to monitor network traffic and notify if any potential threats or attacks are noticed?
A. IPS
B. WAF
C. Firewall
D. IDS
Answer: D (LEAVE A REPLY)
Explanation
An intrusion detection system (IDS) is designed to analyze network packets, compare their contents or characteristics against a set of configurations or signatures, and alert personnel if anything is detected that could constitute a threat or is otherwise designated for alerting.

NEW QUESTION: 509
DLP can be combined with what other security technology to enhance data controls?
Response:
A. Hypervisors
B. SIEM

C. Kerberos
D. DRM
Answer: (SHOW ANSWER)

NEW QUESTION: 510
Proper _____ need to be assigned to each data classification/category.
Response:
A. Metadata
B. Dollar values
C. Security controls
D. Policies
Answer: (SHOW ANSWER)

NEW QUESTION: 511
Which of the cloud cross-cutting aspects relates to the oversight of processes and systems, as well as to ensuring their compliance with specific policies and regulations?
A. Governance
B. Regulatory requirements
C. Service-level agreements
D. Auditability
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Auditing involves reports and evidence that show user activity, compliance with controls and regulations, the systems and processes that run and what they do, as well as information and data access and modification records. A cloud environment adds additional complexity to traditional audits because the cloud customer will not have the same level of access to systems and data as they would in a traditional data center.

NEW QUESTION: 512
Which is the appropriate phase of the cloud data lifecycle for determining the data's classification?

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

NEW QUESTION: 513
What is a serious complication an organization faces from the compliance perspective with international operations?
A. Multiple jurisdictions
B. Different certifications
C. Different operational procedures
D. Different capabilities
Answer: A (LEAVE A REPLY)
When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, which often may not be clearly applicable or may be in contention with each other. These requirements can involve the location of the users and the type of data they enter into systems, the laws governing the organization that owns the application and any regulatory requirements they may have, and finally the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which may be multiple jurisdictions as well. Different certifications would not come into play as a challenge because the major IT and data center certifications are international and would apply to any cloud provider.
Different capabilities and different operational procedures would be mitigated by the organization's selection of a cloud provider and would not be a challenge if an appropriate provider was chosen, regardless of location.

NEW QUESTION: 514
The physical layout of a cloud data center campus should include redundancies of all the following except
_____.
Response:
A. Generator fuel storage
B. HVAC units
C. Generators
D. Points of personnel ingress
Answer: D (LEAVE A REPLY)

NEW QUESTION: 515
A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence.
Which core concept of cloud computing is most related to vendor lock-in?
A. Scalability
B. Interoperability
C. Portability
D. Reversibility
Answer: C (LEAVE A REPLY)
Portability is the ability for a cloud customer to easily move their systems, services, and applications among different cloud providers. By avoiding reliance on proprietary APIs and other vendor-specific cloud features, an organization can maintain flexibility to move among the various cloud providers with greater ease. Reversibility refers to the ability for a cloud customer to quickly and easy remove all their services and data from a cloud provider. Interoperability is the ability to reuse services and components for other applications and uses. Scalability refers to the ability of a cloud environment to add or remove resources to meet current demands.

NEW QUESTION: 516
Which of the following best describes data masking?
A. A method where the last few numbers in a dataset are not obscured. These are often used for authentication.
B. Data masking involves stripping out all similar digits in a string of numbers so as to obscure the original number.
C. A method used to protect prying eyes from data such as social security numbers and credit card data.
D. A method for creating similar but inauthentic datasets used for software testing and user training.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 517
Which type of report is considered for "general" use and does not contain any sensitive information?
A. SOC 3
B. SOC 1
C. SOC 2
D. SAS-70
Answer: A (LEAVE A REPLY)

NEW QUESTION: 518

DLP solutions can aid in deterring loss due to which of the following?
Response:
A. Randomization
B. Natural disaster
C. Device failure
D. Inadvertent disclosure
Answer: D (LEAVE A REPLY)

NEW QUESTION: 519
The WS-Security standards are built around all of the following standards except which one?
A. SAML
B. WDSL
C. XML
D. SOAP
Answer: A (LEAVE A REPLY)
The WS-Security specifications, as well as the WS-Federation system, are built upon XML, WDSL, and SOAP. SAML is a very similar protocol that is used as an alternative to WS.XML, WDSL, and SOAP are all integral to the WS-Security specifications.

NEW QUESTION: 520
Which phase of the cloud data lifecycle represents the first instance where security controls can be implemented?
A. Use
B. Share
C. Store
D. Create
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The store phase occurs immediately after the create phase, and as data is committed to storage structures, the first opportunity for security controls to be implemented is realized. During the create phase, the data is not yet part of a system where security controls can be applied, and although the use and share phases also entail the application of security controls, they are not the first phase where the process occurs.

NEW QUESTION: 521
Which United States law is focused on accounting and financial practices of organizations?
A. Safe Harbor
B. GLBA
C. SOX

D. HIPAA

Answer: (SHOW ANSWER)

The Sarbanes-Oxley (SOX) Act is not an act that pertains to privacy or IT security directly, but rather regulates accounting and financial practices used by organizations. It was passed to protect stakeholders and shareholders from improper practices and errors, and it sets forth rules for compliance, regulated and enforced by the Securities and Exchange Commission (SEC). The main influence on IT systems and operations is the requirements it sets for data retention, specifically in regard to what types of records must be preserved and for how long.

NEW QUESTION: 522

Which of the following best describes SAML?

A. A standard for developing secure application management logistics

B. A standard used for directory synchronization

C. A standard for exchanging usernames and passwords across devices.

D. A standards for exchanging authentication and authorization data between security domains.

Answer: (SHOW ANSWER)

NEW QUESTION: 523

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

A. Monitoring

B. Use of a remote key management system

C. Programming languages used

D. Reliance on physical network controls

Answer: (SHOW ANSWER)

Many organizations in a traditional data center make heavy use of physical network controls for security.

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

NEW QUESTION: 524

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

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

A. Reports

B. Certification

C. Billing
D. Exclusions
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Billing for an audit, or other cost-related items, would not be part of an audit scope statement and would instead be handled prior to the actual audit as part of the contract between the organization and auditors.
Reports, exclusions to the scope of the audit, and required certifications on behalf of the systems or auditors are all crucial elements of an audit scope statement.

NEW QUESTION: 525
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)
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: 526
Audits are either done based on the status of a system or application at a specific time or done as a study over a period of time that takes into account changes and processes. Which of the following pairs matches an audit type that is done over time, along with the minimum span of time necessary for it?
A. SOC Type 2, one year
B. SOC Type 1, one year
C. SOC Type 2, one month
D. SOC Type 2, six months
Answer: D (LEAVE A REPLY)
Explanation

SOC Type 2 audits are done over a period of time, with six months being the minimum duration. SOC Type 1 audits are designed with a scope that's a static point in time, and the other times provided for SOC Type 2 are incorrect.

NEW QUESTION: 527
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 length of time it would take to rebuild the plant
B. The amount of revenue generated by the plant
C. The amount of product the plant creates
D. The rate at which the plant generates revenue
Answer: (SHOW ANSWER)

NEW QUESTION: 528
Because PaaS implementations are so often used for software development, what is one of the vulnerabilities that should always be kept in mind?
A. DoS/DDoS
B. Loss/theft of portable devices
C. Backdoors
D. Malware
Answer: (SHOW ANSWER)

NEW QUESTION: 529
In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?
A. Physical
B. All of the above

C. technological
D. Administrative
Answer: B (LEAVE A REPLY)
Layered defense calls for a diverse approach to security.

NEW QUESTION: 530
Which of the following would NOT be included as input into the requirements gathering for an application or system?
Response:
A. Management
B. Auditors
C. Regulators
D. Users
Answer: B (LEAVE A REPLY)

NEW QUESTION: 531
Which component of ITIL involves handling anything that can impact services for either internal or public users?
A. Incident management
B. Deployment management
C. Problem management
D. Change management
Answer: A (LEAVE A REPLY)
Explanation
Incident management is focused on limiting the impact of disruptions to an organization's services or operations, as well as returning their state to full operational status as soon as possible. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.
Deployment management is a subcomponent of change management and is where the actual code or configuration change is put into place. Change management involves the processes and procedures that allow an organization to make changes to its IT systems and services in a controlled manner.

NEW QUESTION: 532
Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?
A. Regulation
B. Multitenancy
C. Virtualization
D. Resource pooling
Answer: (SHOW ANSWER)

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. Especially within a public cloud model, it is not possible or practical for a cloud provider to alter its services for specific customer demands.
Resource pooling and virtualization within a cloud environment would be the same for all customers, and would not impact certifications that a cloud provider might be willing to pursue. Regulations would form the basis for certification problems and would be a reason for a cloud provider to pursue specific certifications to meet customer requirements.

NEW QUESTION: 533
Key maintenance and security are paramount within a cloud environment due to the widespread use of encryption for both data and transmissions.
Which of the following key-management systems would provide the most robust control over and ownership of the key-management processes for the cloud customer?
A. Remote key management service
B. Local key management service
C. Client key management service
D. Internal key management service
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A remote key management system resides away from the cloud environment and is owned and controlled by the cloud customer. With the use of a remote service, the cloud customer can avoid being locked into a proprietary system from the cloud provider, but also must ensure that service is compatible with the services offered by the cloud provider. A local key management system resides on the actual servers using the keys, which does not provide optimal security or control over them. Both the terms internal key management service and client key management service are provided as distractors.

NEW QUESTION: 534
In the cloud motif, the data processor is usually:
A. The party that assigns access rights
B. The cloud access security broker
C. The cloud customer
D. The cloud provider
Answer: D (LEAVE A REPLY)

NEW QUESTION: 535

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

NEW QUESTION: 536
Which attribute of data poses the biggest challenge for data discovery?
A. Labels
B. Quality
C. Volume
D. Format
Answer: (SHOW ANSWER)
Explanation
The main problem when it comes to data discovery is the quality of the data that analysis is being performed against. Data that is malformed, incorrectly stored or labeled, or incomplete makes it very difficult to use analytical tools against.

NEW QUESTION: 537
Which if the following is NOT one of the three components of a federated identity system transaction?
A. User
B. Relying party
C. Identity provider
D. Proxy relay
Answer: (SHOW ANSWER)

NEW QUESTION: 538
Managed cloud services exist because the service is less expensive for each customer than creating the same services for themselves in a legacy environment.
Using a managed service allows the customer to realize significant cost savings through the reduction of _____.
Response:
A. Security controls
B. Data
C. Personnel
D. Risk

Answer: C (LEAVE A REPLY)

NEW QUESTION: 539
Which of the following is an example of useful and sufficient data masking of the string "CCSP"?
Response:
A. PSCC
B. 3X91
C. TtLp
D. XCSP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 540
Which format is the most commonly used standard for exchanging information within a federated identity system?
A. XML
B. HTML
C. SAML
D. JSON
Answer: C (LEAVE A REPLY)
Explanation
Security Assertion Markup Language (SAML) is the most common data format for information exchange within a federated identity system. It is used to transmit and exchange authentication and authorization data.XML is similar to SAML, but it's used for general-purpose data encoding and labeling and is not used for the exchange of authentication and authorization data in the way that SAML is for federated systems. JSON is used similarly to XML, as a text-based data exchange format that typically uses attribute-value pairings, but it's not used for authentication and authorization exchange. HTML is used only for encoding web pages for web browsers and is not used for data exchange--and certainly not in a federated system.

NEW QUESTION: 541
Why are PaaS environments at a higher likelihood of suffering backdoor vulnerabilities?
A. They are scalable.
B. They rely on virtualization.
C. They are often used for software development.
D. They have multitenancy.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 542
Which of the following technologies is used to monitor network traffic and notify if any potential threats or attacks are noticed?
A. IPS
B. WAF
C. Firewall
D. IDS
Answer: D (LEAVE A REPLY)
An intrusion detection system (IDS) is designed to analyze network packets, compare their contents or characteristics against a set of configurations or signatures, and alert personnel if anything is detected that could constitute a threat or is otherwise designated for alerting.

NEW QUESTION: 543
Which of the following represents a control on the maximum amount of resources that a single customer, virtual machine, or application can consume within a cloud environment?
A. Share
B. Reservation
C. Provision
D. Limit
Answer: D (LEAVE A REPLY)
Limits are put in place to enforce a maximum on the amount of memory or processing a cloud customer can use. This can be done either on a virtual machine or as a comprehensive whole for a customer, and is meant to ensure that enormous cloud resources cannot be allocated or consumed by a single host or customer to the detriment of other hosts and customers.

NEW QUESTION: 544
Data transformation in a cloud environment should be of great concern to organizations considering cloud migration because _____ could affect data classification processes/implementations.
A. Multitenancy
B. Remote access

C. Physical distance
D. Virtualization
Answer: (SHOW ANSWER)

NEW QUESTION: 545
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
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: 546
What does static application security testing (SAST) offer as a tool to the testers?
A. Production system scanning
B. Injection attempts
C. Source code access
D. Live testing
Answer: C (LEAVE A REPLY)
Explanation
Static application security testing (SAST) is conducted with knowledge of the system, including source code, and is done against offline systems.

NEW QUESTION: 547
Which of the following is not a feature of SAST?
A. "White-box" testing
B. Highly skilled, often expensive outside consultants
C. Team-building efforts
D. Source code review
Answer: C (LEAVE A REPLY)

NEW QUESTION: 548
Configurations and policies for a system can come from a variety of sources and take a variety of formats. Which concept pertains to the application of a set of configurations and policies that is applied to all systems or a class of systems?

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

NEW QUESTION: 549
Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like:
Response:
A. XSS and SQL injection
B. Password cracking
C. Ransomware
D. Syn floods
Answer: A (LEAVE A REPLY)

NEW QUESTION: 550
From a legal perspective, what is the most important first step after an eDiscovery order has been received by the cloud provider?
A. Notification
B. Key identification
C. Data collection
D. Virtual image snapshots
Answer: (SHOW ANSWER)
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: 551
Cryptographic keys for encrypted data stored in the cloud should be _____ .
A. Not stored with the cloud provider.
B. Generated with redundancy
C. At least 128 bits long
D. Split into groups

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

NEW QUESTION: 552
Which protocol, as a part of TLS, handles the actual secure communications and transmission of data?
A. Negotiation
B. Handshake
C. Transfer
D. Record
Answer: (SHOW ANSWER)
Explanation
The TLS record protocol is the actual secure communications method for transmitting data; it's responsible for encrypting and authenticating packets throughout their transmission between the parties, and in some cases it also performs compression. The TLS handshake protocol is what negotiates and establishes the TLS connection between two parties and enables the secure communications channel to then handle data transmissions.
Negotiation and transfer are not protocols under TLS.

NEW QUESTION: 553
You are the IT security manager for a video game software development company. Which of the following is most likely to be your primary concern on a daily basis?
A. Security flaws in your products
B. Regulatory compliance
C. Security flaws in your organization
D. Health and human safety
Answer: C (LEAVE A REPLY)

NEW QUESTION: 554
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing.
According to the CSA, what aspect of managed cloud services makes the threat of malicious insiders so alarming?
A. Multitenancy
B. Flexibility
C. Scalability
D. Metered service
Answer: A (LEAVE A REPLY)

NEW QUESTION: 555
Jurisdictions have a broad range of privacy requirements pertaining to the handling of personal data and information.
Which jurisdiction requires all storage and processing of data that pertains to its citizens to be done on hardware that is physically located within its borders?
A. Japan
B. United States
C. European Union
D. Russia
Answer: D (LEAVE A REPLY)
The Russian government requires all data and processing of information about its citizens to be done solely on systems and applications that reside within the physical borders of the country.
The United States, European Union, and Japan focus their data privacy laws on requirements and methods for the protection of data, rather than where the data physically resides.

NEW QUESTION: 556
What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?
A. Proxy
B. Bastion
C. Honeypot
D. WAF
Answer: (SHOW ANSWER)
A bastion host is a server that is fully exposed to the public Internet, but is extremely hardened to prevent attacks and is usually dedicated for a specific application or usage; it is not something that will serve multiple purposes. This singular focus allows for much more stringent security hardening and monitoring.

NEW QUESTION: 557
Data masking can be used to provide all of the following functionality, except:

A. Secure remote access
B. test data in sandboxed environments
C. Authentication of privileged users
D. Enforcing least privilege
Answer: C (LEAVE A REPLY)
Data masking does not support authentication in any way. All the others are excellent use cases for data masking.

NEW QUESTION: 558
Which security concept is based on preventing unauthorized access to data while also ensuring that it is accessible to those authorized to use it?
A. Integrity
B. Availability
C. Confidentiality
D. Nonrepudiation
Answer: C (LEAVE A REPLY)
Explanation
The main goal of confidentiality is to ensure that sensitive information is not made available or leaked to parties that should not have access to it, while at the same time ensuring that those with appropriate need and authorization to access it can do so in a manner commensurate with their needs and confidentiality requirements.

NEW QUESTION: 559
What is the first stage of the cloud data lifecycle where security controls can be implemented?
A. Use
B. Store
C. Share
D. Create
Answer: B (LEAVE A REPLY)
The "store" phase of the cloud data lifecycle, which typically occurs simultaneously with the "create" phase, or immediately thereafter, is the first phase where security controls can be implemented. In most case, the manner in which the data is stored will be based on its classification.

NEW QUESTION: 560
Which technology is NOT commonly used for security with data in transit?
A. DNSSEC
B. IPsec
C. VPN
D. HTTPS

Answer: A (LEAVE A REPLY)
Explanation
DNSSEC relates to the integrity of DNS resolutions and the prevention of spoofing or redirection, and does not pertain to the actual security of transmissions or the protection of data.

NEW QUESTION: 561
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: 562
From a security perspective, automation of configuration aids in _____.
Response:
A. Reducing potential attack vectors
B. Enhancing performance
C. Reducing need for administrative personnel
D. Increasing ease of use of the systems
Answer: A (LEAVE A REPLY)

NEW QUESTION: 563
What type of masking strategy involves replacing data on a system while it passes between the data and application layers?
A. Dynamic
B. Static
C. Replication
D. Duplication
Answer: A (LEAVE A REPLY)
With dynamic masking, production environments are protected with the masking process being implemented between the application and data layers of the application. This allows for a masking translation to take place live in the system and during normal application processing of data.

NEW QUESTION: 564
The European Union is often considered the world leader in regard to the privacy of personal data and has declared privacy to be a "human right." In what year did the EU first assert this principle?
A. 1995
B. 2000
C. 2010
D. 1999
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The EU passed Directive 95/46 EC in 1995, which established data privacy as a human right. The other years listed are incorrect.

NEW QUESTION: 565
Being in a cloud environment, cloud customers lose a lot of insight and knowledge as to how their data is stored and their systems are deployed.
Which concept from the ISO/IEC cloud standards relates to the necessity of the cloud provider to inform the cloud customer on these issues?
A. Disclosure
B. Transparency
C. Openness
D. Documentation
Answer: B (LEAVE A REPLY)
Explanation
Transparency is the official process by which a cloud provider discloses insight and information into its configurations or operations to the appropriate audiences. Disclosure, openness, and documentation are all terms that sound similar to the correct answer, but none of them is the correct term in this case.

NEW QUESTION: 566
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/Reference:
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: 567
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: A (LEAVE A REPLY)
Explanation
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: 568
What does static application security testing (SAST) offer as a tool to the testers that makes it unique compared to other common security testing methodologies?
A. Live testing
B. Source code access
C. Production system scanning
D. Injection attempts
Answer: B (LEAVE A REPLY)
Static application security testing (SAST) is conducted against offline systems with previous knowledge of them, including their source code. Live testing is not part of static testing but rather is associated with dynamic testing. Production system scanning is not appropriate because static testing is done against offline systems. Injection attempts are done with many different types of testing and are not unique to one particular type. It is therefore not the best answer to the question.

NEW QUESTION: 569

What provides the information to an application to make decisions about the authorization level appropriate when granting access?

A. User

B. Relying party

C. Federation

D. Identity Provider

Answer: (SHOW ANSWER)

Explanation

Upon successful user authentication, the identity provider gives information about the user to the relying party that it needs to make authorization decisions for granting access as well as the level of access needed.

NEW QUESTION: 570

Which of the following is not an enforceable governmental request?

A. Affidavit

B. Warrant

C. Subpoena

D. Court order

Answer: (SHOW ANSWER)

NEW QUESTION: 571

During which stage of the SDLC process should security be consulted and begin its initial involvement?

A. Testing

B. Design

C. Requirement gathering

D. Development

Answer: C (LEAVE A REPLY)

NEW QUESTION: 572

Which of the following roles is responsible for overseeing customer relationships and the processing of financial transactions?

A. Cloud service manager
B. Cloud service deployment
C. Cloud service business manager
D. Cloud service operations manager
Answer: C (LEAVE A REPLY)
Explanation
The cloud service business manager is responsible for overseeing business plans and customer relationships as well as processing financial transactions.

NEW QUESTION: 573
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: 574
Which of the following is the best example of a key component of regulated PII?
A. Audit rights of subcontractors
B. Items that should be implemented
C. PCI DSS
D. Mandatory breach reporting
Answer: D (LEAVE A REPLY)
Explanation
Mandatory breach reporting is the best example of regulated PII components. The rest are generally considered components of contractual PII.

NEW QUESTION: 575
_____ is perhaps the main external factor driving IAM efforts.
Response:
A. The evolving threat landscape
B. Regulation
C. Business need

D. Monetary value
Answer: (SHOW ANSWER)