ISC.CCSP.v2022-08-08.q191

Exam Code:	CCSP
Exam Name:	Certified Cloud Security Professional
Certification Provider:	ISC
Free Question Number:	191
Version:	v2022-08-08
# of views:	2688
# of Questions views:	1910
https://www.exam-tests.com/CCSP-exam/ISC.CCSP.v2022-08-08.q191.html	

NEW QUESTION: 1
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: D (LEAVE A REPLY)
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: 2
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)

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: 3
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: 4
The GAPP framework was developed through a joint effort between the major Canadian and American professional accounting associations in order to assist their members with managing and preventing risks to the privacy of their data and customers.
Which of the following is the meaning of GAPP?
A. General accounting personal privacy
B. Generally accepted privacy practices
C. General accounting privacy policies
D. Generally accepted privacy principles
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
Which of the following is NOT a function performed by the handshake protocol of TLS?
A. Key exchange

B. Encryption
C. Negotiation of connection
D. Establish session ID
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The handshake protocol negotiates and establishes the connection as well as handles the key exchange and establishes the session ID. It does not perform the actual encryption of data packets.

NEW QUESTION: 6
The REST API is a widely used standard for communications of web-based services between clients and the servers hosting them.
Which protocol does the REST API depend on?
A. HTTP
B. SSH
C. SAML
D. XML
Answer: A (LEAVE A REPLY)
Representational State Transfer (REST) is a software architectural scheme that applies the components, connectors, and data conduits for many web applications used on the Internet. It uses and relies on the HTTP protocol and supports a variety of data formats. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data.
Secure Shell client (SSH) is a secure method for allowing remote login to systems over a network.

NEW QUESTION: 7
Which of the following technologies is NOT commonly used for accessing systems and services in a cloud environment in a secure manner?
A. KVM
B. HTTPS
C. VPN
D. TLS
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A keyboard-video-mouse (KVM) system is commonly used for directly accessing server terminals in a data center. It is not a method that would be possible within a cloud environment, primarily due to the use virtualized systems, but also because only the cloud

provider's staff would be allowed the physical access to hardware systems that's provided by a KVM. Hypertext Transfer Protocol Secure (HTTPS), virtual private network (VPN), and Transport Layer Security (TLS) are all technologies and protocols that are widely used with cloud implementations for secure access to systems and services.

NEW QUESTION: 8
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/Reference:
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: 9
Fiber-optic lines are considered part of layer _____ of the OSI model.
Response:
A. 7
B. 5
C. 1
D. 3
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
Which aspect of cloud computing makes data classification even more vital than in a traditional data center?
A. Interoperability
B. Virtualization
C. Multitenancy
D. Portability
Answer: C (LEAVE A REPLY)
With multiple tenants within the same hosting environment, any failure to properly classify data may lead to potential exposure to other customers and applications within the same environment.

NEW QUESTION: 11
Which of the following is NOT one of the cloud computing activities, as outlined in ISO/IEC 17789?
A. Cloud service administrator
B. Cloud service customer
C. Cloud service provider
D. Cloud service partner
Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
Which SSAE 16 audit report is simply an attestation of audit results?
A. SOC 3
B. SOC 1
C. SOC 2, Type 1
D. SOC 2, Type 2
Answer: A (LEAVE A REPLY)

NEW QUESTION: 13
Which ISO/IEC standards set documents the cloud definitions for staffing and official roles?
Response:
A. ISO/IEC 27001
B. ISO/IEC 27040
C. ISO/IEC 17789
D. ISO/IEC 17788
Answer: D (LEAVE A REPLY)

NEW QUESTION: 14
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: 15
Which of the following is NOT considered a type of data loss?
A. Data corruption
B. Stolen by hackers
C. Accidental deletion
D. Lost or destroyed encryption keys
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The exposure of data by hackers is considered a data breach. Data loss focuses on the data availability rather than security. Data loss occurs when data becomes lost, unavailable, or destroyed, when it should not have been.

NEW QUESTION: 16
What is the only data format permitted with the SOAP API?
A. HTML
B. SAML
C. XSML
D. XML
Answer: (SHOW ANSWER)
The SOAP protocol only supports the XML data format.

NEW QUESTION: 17
Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?
Response:
A. Delineating biometric catalogs

B. Mapping to existing access control lists (ACLs)
C. Prohibiting unauthorized transposition
D. Preventing multifactor authentication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "using components with known vulnerabilities." Why would an organization ever use components with known vulnerabilities to create software?
Response:
A. A component might have a hidden vulnerability.
B. The particular vulnerabilities only exist in a context not being used by developers.
C. The organization is insured.
D. Some vulnerabilities only exist in foreign countries.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
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: 20
What must SOAP rely on for security?
A. Encryption
B. Tokenization
C. TLS
D. SSL
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:
Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for passing data, and it must rely on the encryption of those data packages for security.

NEW QUESTION: 21
While an audit is being conducted, which of the following could cause management and the auditors to change the original plan in order to continue with the audit?
A. Impact on systems
B. Software version changes
C. Cost overruns
D. Regulatory changes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
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/Reference:
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: 23
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

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: 24
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)
Explanation
Options A and C are also correct, but included in B, making B the best choice. D is incorrect, because we don't want unauthorized users gaining access.

NEW QUESTION: 25
All of the following are identity federation standards commonly found in use today except _____.
Response:
A. WS-Federation
B. OpenID
C. OAuth
D. PGP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 26
Which of the following are cloud computing roles?
A. Cloud service broker and user
B. Cloud customer and financial auditor
C. CSP and backup service provider

D. Cloud service auditor and object

Answer: C (LEAVE A REPLY)

Explanation

The following groups form the key roles and functions associated with cloud computing. They do not constitute an exhaustive list but highlight the main roles and functions within cloud computing:

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

May also resell cloud services.

- Cloud service auditor: Third-party organization that verifies attainment of SLAs.

NEW QUESTION: 27

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

Response:

A. Accepting

B. Mitigating

C. Enveloping

D. Transferring

Answer: C (LEAVE A REPLY)

NEW QUESTION: 28

Impact resulting from risk being realized is often measured in terms of _____.

A. Amount of property lost

B. Number of people affected

C. Amount of data lost

D. Money

Answer: D (LEAVE A REPLY)

NEW QUESTION: 29

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: 30

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

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: 31

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: 32
Halon is now illegal to use for data center fire suppression. What is the reason it was outlawed?
Response:
A. It does not adequately suppress fires.
B. It poses a threat to health and human safety when deployed.
C. It causes undue damage to electronic systems.
D. It can harm the environment.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 33
FM-200 has all the following properties except _____.
Response:
A. It may deplete the Earth's ozone layer
B. It's nontoxic at levels used for fire suppression
C. It does not leave a film or coagulant after use
D. It's gaseous at room temperature
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
When designing a cloud data center, which of the following aspects is not necessary to ensure continuity of operations during contingency operations?
A. Broadband data connection
B. Access to clean water
C. Physical access to the data center
D. Extended battery backup

Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
What is the primary reason that makes resolving jurisdictional conflicts complicated?
A. Different technology standards
B. Costs
C. Language barriers
D. Lack of international authority
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
With international operations, systems ultimately cross many jurisdictional boundaries, and many times, they conflict with each other. The major hurdle to overcome for an organization is the lack of an ultimate international authority to mediate such conflicts, with a likely result of legal efforts in each jurisdiction.

NEW QUESTION: 36
In which cloud service model is the customer required to maintain the OS?
A. Iaas
B. CaaS
C. PaaS
D. SaaS
Answer: (SHOW ANSWER)
Explanation
In IaaS, the service is bare metal, and the customer has to install the OS and the software; the customer then is responsible for maintaining that OS. In the other models, the provider installs and maintains the OS.

NEW QUESTION: 37
Which of the following provides assurance, to a predetermined acceptable level of certainty, that an entity is indeed who they claim to be?
A. Authentication
B. Identification
C. Proofing
D. Authorization
Answer: (SHOW ANSWER)
Explanation
Authentication goes a step further than identification by providing a means for proving an entity's identification. Authentication is most commonly done through mechanisms such as passwords. Identification involves ascertaining who the entity is, but without a means of proving it, such as a name or user ID.

Authorization occurs after authentication and sets access permissions and other privileges within a system or application for the user. Proofing is not a term that is relevant to the question.

NEW QUESTION: 38
From a legal perspective, what is the most important first step after an eDiscovery order has been received by the cloud provider?
A. Notification
B. Key identification
C. Data collection
D. Virtual image snapshots
Answer: A (LEAVE A REPLY)
The contract should include requirements for notification by the cloud provider to the cloud customer upon the receipt of such an order. This serves a few important purposes. First, it keeps communication and trust open between the cloud provider and cloud customers. Second, and more importantly, it allows the cloud customer to potentially challenge the order if they feel they have the grounds or desire to do so.

NEW QUESTION: 39
What does the management plane typically utilize to perform administrative functions on the hypervisors that it has access to?
A. Scripts
B. RDP
C. APIs
D. XML
Answer: C (LEAVE A REPLY)
Explanation
The functions of the management plane are typically exposed as a series of remote calls and function executions and as a set of APIs. These APIs are typically leveraged through either a client or a web portal, with the latter being the most common.

NEW QUESTION: 40
_____ is the legal concept whereby a cloud customer is held to a reasonable expectation for providing security of its users' and clients' privacy data.
A. Reciprocity
B. Due care
C. Due diligence
D. Liability
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41

You were recently hired as a project manager at a major university to implement cloud services for the academic and administrative systems. Because the load and demand for services at a university are very cyclical in nature, commensurate with the academic calendar, which of the following aspects of cloud computing would NOT be a primary benefit to you?

A. Measured service

B. Broad network access

C. Resource pooling

D. On-demand self-service

Answer: B (LEAVE A REPLY)

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: 42

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

A. Audit rights of subcontractors

B. PCI DSS

C. Items that should be implemented

D. Mandatory breach reporting

Answer: D (LEAVE A REPLY)

NEW QUESTION: 43

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

A. SSAE 16

B. SOC 2

C. SOC 1

D. SOC 3

Answer: C (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 44

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

A. Law enforcement notification

B. User punishment

C. Device tracking

D. Credential revocation

Answer: D (LEAVE A REPLY)

NEW QUESTION: 45

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/Reference:

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: 46

Where is a DLP solution generally installed when utilized for monitoring data in transit?

A. Network perimeter

B. Database server

C. Application server

D. Web server

Answer: A (LEAVE A REPLY)

To monitor data in transit, a DLP solution would optimally be installed at the network perimeter, to ensure that data leaving the network through various protocols conforms to security controls and policies. An application server or a web server would be more appropriate for monitoring data in use, and a database server would be an example of a location appropriate for monitoring data at rest.

NEW QUESTION: 47
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: (SHOW ANSWER)
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: 48
Which component of ITIL pertains to planning, coordinating, executing, and validating changes and rollouts to production environments?
A. Release management
B. Availability management
C. Problem management
D. Change management
Answer: A (LEAVE A REPLY)
Release management involves planning, coordinating, executing, and validating changes and rollouts to the production environment. Change management is a higher-level component than release management and also involves stakeholder and management approval, rather than specifically focusing the actual release itself. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION: 49
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: 50
On large distributed systems with pooled resources, cloud computing relies on extensive orchestration to maintain the environment and the constant provisioning of resources. Which of the following is crucial to the orchestration and automation of networking resources within a cloud?
A. DNSSEC
B. DNS
C. DCOM
D. DHCP
Answer: D (LEAVE A REPLY)
The Dynamic Host Configuration Protocol (DHCP) automatically configures network settings for a host so that these settings do not need to be configured on the host statically. Given the rapid and programmatic provisioning of resources within a cloud environment, this capability is crucial to cloud operations. Both DNS and its security-integrity extension DNSSEC provide name resolution to IP addresses, but neither is used for the configuration of network settings on a host.
DCOM refers to the Distributed Component Object Model, which was developed by Microsoft as a means to request services across a network, and is not used for network configurations at all.

NEW QUESTION: 51
Which of the following cloud aspects complicates eDiscovery?
A. Resource pooling
B. On-demand self-service
C. Multitenancy
D. Measured service
Answer: (SHOW ANSWER)
Explanation/Reference:
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: 52
Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.

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

A. HIPAA

B. SOX

C. FISMA

D. PCI DSS

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry-regulatory standard, not a governmental one. The Sarbanes-Oxley Act (SOX) was passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders. The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

NEW QUESTION: 53

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

A. Data loss

B. Denial of service

C. Data breach

D. Distributed

Answer: B (LEAVE A REPLY)

Explanation

Any application can be a possible target of denial-of-service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for non-authenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks.

NEW QUESTION: 54

What is one of the reasons a baseline might be changed?

A. Numerous change requests

B. To reduce redundancy

C. Natural disaster

D. Power fluctuation

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

If the CMB is receiving numerous change requests to the point where the amount of requests would drop by modifying the baseline, then that is a good reason to change the baseline. None of the other reasons should involve the baseline at all.

NEW QUESTION: 55
Which of the following standards primarily pertains to cabling designs and setups in a data center?
A. IDCA
B. BICSI
C. NFPA
D. Uptime Institute
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The standards put out by Building Industry Consulting Service International (BICSI) primarily cover complex cabling designs and setups for data centers, but also include specifications on power, energy efficiency, and hot/cold aisle setups.

NEW QUESTION: 56
Which security concept would business continuity and disaster recovery fall under?
A. Confidentiality
B. Availability
C. Fault tolerance
D. Integrity
Answer: B (LEAVE A REPLY)
Explanation
Disaster recovery and business continuity are vital concerns with availability. If data is destroyed or compromised, having regular backup systems in place as well as being able to perform disaster recovery in the event of a major or widespread problem allows operations to continue with an acceptable loss of time and data to management. This also ensures that sensitive data is protected and persisted in the event of the loss or corruption of data systems or physical storage systems.

NEW QUESTION: 57
Which of the following is a method for apportioning resources that involves setting guaranteed minimums for all tenants/customers within the environment?
A. Cancellations
B. Shares
C. Reservations
D. Limits
Answer: (SHOW ANSWER)

NEW QUESTION: 58
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)
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: 59
In order to comply with regulatory requirements, which of the following secure erasure methods would be available to a cloud customer using volume storage within the IaaS service model?
A. Demagnetizing
B. Shredding
C. Degaussing
D. Cryptographic erasure
Answer: D (LEAVE A REPLY)
Explanation
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: 60
What could be the result of failure of the cloud provider to secure the hypervisor in such a way that one user on a virtual machine can see the resource calls of another user's virtual machine?
Response:
A. Social engineering
B. Inference attacks
C. Physical intrusion
D. Unauthorized data disclosure
Answer: B (LEAVE A REPLY)

NEW QUESTION: 61

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

A. Unvalidated redirects and forwards

B. Insecure direct object references

C. Security miscomfiguration

D. Sensitive data exposure

Answer: A (LEAVE A REPLY)

Explanation

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: 62

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)

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: 63
What is the best source for information about securing a physical asset's BIOS?
A. Security policies
B. Manual pages
C. Vendor documentation
D. Regulations
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Vendor documentation from the manufacturer of the physical hardware is the best source of best practices for securing the BIOS.

NEW QUESTION: 64
Which type of testing uses the same strategies and toolsets that hackers would use?
A. Penetration
B. Dynamic
C. Static
D. Malicious
Answer: (SHOW ANSWER)
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: 65
Who is the entity identified by personal data?
Response:
A. The data subject
B. The data processor
C. The data owner
D. The data custodian
Answer: (SHOW ANSWER)

NEW QUESTION: 66
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
Print spooling is not a metric for system performance; all the rest are.

NEW QUESTION: 67
Which regulatory system pertains to the protection of healthcare data?
A. HIPAA
B. HAS
C. HITECH
D. HFCA
Answer: A (LEAVE A REPLY)
Explanation
The Health Insurance Portability and Accountability Act (HIPAA) sets stringent requirements in the United States for the protection of healthcare records.

NEW QUESTION: 68
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: 69
What is the most secure form of code testing and review?
Response:
A. Combination of open source and proprietary
B. Neither open source nor proprietary
C. Proprietary/internal

D. Open source
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70
Countermeasures for protecting cloud operations against internal threats include all of the following except:
A. Mandatory vacation
B. Least privilege
C. Separation of duties
D. Conflict of interest
Answer: D (LEAVE A REPLY)
Conflict of interest is a threat, not a control.

NEW QUESTION: 71
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: (SHOW ANSWER)
Explanation
The value of data itself has nothing to do with it being considered a part of contractual

NEW QUESTION: 72
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. Hot aisle containment
B. Thermo-optimized
C. HVAC modulated
D. Cold aisle containment
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which of the following contract terms most incentivizes the cloud provider to meet the requirements listed in the SLA?
A. Regulatory oversight
B. Financial penalties
C. Performance details
D. Desire to maintain customer satisfaction
Answer: (SHOW ANSWER)

NEW QUESTION: 74
In addition to battery backup, a UPS can offer which capability?
A. Breach alert
B. Confidentiality
C. Communication redundancy
D. Line conditioning
Answer: D (LEAVE A REPLY)
A UPS can provide line conditioning, adjusting power so that it is optimized for the devices it serves and smoothing any power fluctuations; it does not offer any of the other listed functions.

NEW QUESTION: 75
To protect data on user devices in a BYOD environment, the organization should consider requiring all the following, except:
A. Multifactor authentication
B. DLP agents
C. Two-person integrity
D. Local encryption
Answer: C (LEAVE A REPLY)
Although all the other options are ways to harden a mobile device, two-person integrity is a concept that has nothing to do with the topic, and, if implemented, would require everyone in your organization to walk around in pairs while using their mobile devices.

NEW QUESTION: 76
Which of the following threats from the OWASP Top Ten is the most difficult for an organization to protect against?
Response:
A. Malicious insiders
B. Account hijacking
C. Advanced persistent threats
D. Denial of service
Answer: (SHOW ANSWER)

NEW QUESTION: 77
You are working for a cloud service provider and receive an eDiscovery order pertaining to one of your customers.
Which of the following would be the most appropriate action to take first?
A. Take a shapshot of the virtual machines
B. Escrow the encryption keys
C. Copy the data
D. Notify the customer
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
When a cloud service provider receives an eDiscovery order pertaining to one of their customers, the first action they must take is to notify the customer. This allows the customer to be aware of what was received, as well as to conduct a review to determine if any challenges are necessary or warranted. Taking snapshots of virtual machines, copying data, and escrowing encryption keys are all processes involved in the actual collection of data and should not be performed until the customer has been notified of the request.

NEW QUESTION: 78
DLP can be combined with what other security technology to enhance data controls?
A. SIEM
B. Hypervisors
C. DRM
D. Kerberos
Answer: C (LEAVE A REPLY)
Explanation
DLP can be combined with DRM to protect intellectual property; both are designed to deal with data that falls into special categories. SIEMs are used for monitoring event logs, not live data movement. Kerberos is an authentication mechanism. Hypervisors are used for virtualization.

NEW QUESTION: 79
Deviations from the baseline should be investigated and _____.
A. Revealed
B. Documented
C. Encouraged
D. Enforced
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 80
Many tools and technologies are available for securing or monitoring data in transit within a data center, whether it is a traditional data center or a cloud.
Which of the following is NOT a technology for securing data in transit?
A. VPN
B. TLS
C. DNSSEC
D. HTTPS
Answer: C (LEAVE A REPLY)
Explanation
Explanation:
DNSSEC is an extension of the normal DNS protocol that enables a system to verify the integrity of a DNS query resolution by signing it from the authoritative source and verifying the signing chain. It is not used for securing data transmissions or exchanges. HTTPS is the most common method for securing web service and data calls within a cloud, and TLS is the current standard for encrypting HTTPS traffic. VPNs are widely used for securing data transmissions and service access.

NEW QUESTION: 81
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)
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: 82
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: (SHOW ANSWER)
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: 83
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "sensitive data exposure." Which of these is a technique to reduce the potential for a sensitive data exposure?
Response:
A. Extensive user training on proper data handling techniques
B. Ensuring the use of utility backup power supplies
C. Roving security guards
D. Advanced firewalls inspecting all inbound traffic, to include content-based screening
Answer: A (LEAVE A REPLY)

NEW QUESTION: 84
Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider?
Response:
A. SOC 3
B. SOC 2 Type 2
C. SOC 1 Type 1
D. SOC 1 Type 2
Answer: A (LEAVE A REPLY)

NEW QUESTION: 85
Best practices for key management include all of the following, except:
A. Ensure multifactor authentication
B. Pass keys out of band
C. Have key recovery processes
D. Maintain key security
Answer: (SHOW ANSWER)
We should do all of these except for requiring multifactor authentication, which is pointless in key management.

NEW QUESTION: 86
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: 87
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: 88
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: 89
From a security perspective, automation of configuration aids in _____.
A. Reducing potential attack vectors
B. Increasing ease of use of the systems
C. Reducing need for administrative personnel
D. Enhancing performance
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?
A. Six months
B. One month
C. One year
D. One week
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
SOC Type 2 reports are focused on the same policies and procedures, as well as their effectiveness, as SOC Type 1 reports, but are evaluated over a period of at least six consecutive months, rather than a finite point in time.

NEW QUESTION: 91
Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?
A. Data
B. Cash
C. Systems
D. Personnel
Answer: B (LEAVE A REPLY)

NEW QUESTION: 92
Which of the following is characterized by a set maximum capacity?
Response:
A. A secret-sharing-made-short (SSMS) bit-splitting implementation
B. A tightly coupled cloud storage cluster
C. A public-key infrastructure
D. A loosely coupled cloud storage cluster
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
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: 94
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: (SHOW ANSWER)
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: 95
Which security certification serves as a general framework that can be applied to any type of system or application?
Response:
A. PCI DSS
B. ISO/IEC 27001
C. NIST SP 800-53
D. FIPS 140-2
Answer: B (LEAVE A REPLY)

NEW QUESTION: 96
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)
Explanation
Sandboxing involves the segregation and isolation of information or processes from other information or processes within the same system or application, typically for security concerns. Sandboxing is generally used for data isolation (for example, keeping different communities and populations of users isolated from others with similar data). In IT terminology, pooling typically means bringing together and consolidating resources or services, not segregating or separating them. Cell blocking and fencing are both erroneous terms.

NEW QUESTION: 97
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: 98
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)
Explanation
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: 99
Of the following, which is probably the most significant risk in a managed cloud environment?
Response:
A. Physical attack on the utility service lines
B. Guest escape
C. DDoS
D. Management plane breach
Answer: D (LEAVE A REPLY)

NEW QUESTION: 100
Which of the following in a federated environment is responsible for consuming authentication tokens?
Response:
A. Authentication provider
B. Relying party
C. Cloud services broker
D. Identity provider
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
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)
Explanation
The management plane will have broad administrative access to all host systems throughout an environment; as such, it represents the most pressing security concerns. A compromise of the management plane can directly lead to compromises of any other systems within the environment. Although hypervisors represent a significant security concern to an environment because their compromise would expose any virtual systems hosted within them, the management plane is a better choice in this case because it controls multiple hypervisors. Encryption and object storage both represent lower-level security concerns.

NEW QUESTION: 102
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: (SHOW ANSWER)
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: 103
Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?
A. Six months
B. One month
C. One year
D. One week
Answer: A (LEAVE A REPLY)
SOC Type 2 reports are focused on the same policies and procedures, as well as their effectiveness, as SOC Type 1 reports, but are evaluated over a period of at least six consecutive months, rather than a finite point in time.

NEW QUESTION: 104
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: 105
When is a virtual machine susceptible to attacks while a physical server in the same state would not be?
A. When it is behind a WAF
B. When it is behind an IPS
C. When it is not patched
D. When it is powered off
Answer: D (LEAVE A REPLY)
Explanation
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: 106
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: 107
Three central concepts define what type of data and information an organization is responsible for pertaining to eDiscovery.
Which of the following are the three components that comprise required disclosure?
A. Possession, ownership, control
B. Ownership, use, creation
C. Control, custody, use
D. Possession, custody, control
Answer: D (LEAVE A REPLY)
Data that falls under the purview of an eDiscovery request is that which is in the possession, custody, or control of the organization. Although this is an easy concept in a traditional data center, it can be difficult to distinguish who actually possesses and controls the data in a cloud environment due to multitenancy and resource pooling. Although these options provide similar- sounding terms, they are ultimately incorrect.

NEW QUESTION: 108
Which of the following would NOT be used to determine the classification of data?
Response:
A. Creator
B. Metadata
C. Future use
D. PII
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
The use of which of the following technologies will NOT require the security dependency of an operating system, other than its own?
A. Type 2 hypervisor
B. Virtual machine
C. Type 1 hypervisor
D. Management plane

Answer: C (LEAVE A REPLY)

NEW QUESTION: 110
Which kind of SSAE audit report is most beneficial for a cloud customer, even though it's unlikely the cloud provider will share it?
A. SOC 3
B. SOC 1 Type 2
C. SOC 2 Type 2
D. SOC 1 Type 1
Answer: C (LEAVE A REPLY)
The SOC 3 is the least detailed, so the provider is not concerned about revealing it. The SOC 1 Types 1 and 2 are about financial reporting and not relevant. The SOC 2 Type 2 is much more detailed and will most likely be kept closely held by the provider.

NEW QUESTION: 111
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
In order to get truly holistic coverage of your environment, you should be sure to include _____ as a step in the deployment process.
Response:
A. Getting signed user agreements from all users
B. Installation of the solution on all assets in the cloud data center
C. All of your customers to install the tool
D. Adoption of the tool in all routers between your users and the cloud provider
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?
A. HIPAA
B. The contract
C. Statutes
D. Security control matrix
Answer: B (LEAVE A REPLY)
The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable. The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

NEW QUESTION: 113
Tokenization requires two distinct _____ .
A. Authentication factors
B. Personnel
C. Databases
D. Encryption
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
In order to implement tokenization, there will need to be two databases: the database containing the raw, original data, and the token database containing tokens that map to original data. Having two-factor authentication is nice, but certainly not required. Encryption keys are not necessary for tokenization. Two- person integrity does not have anything to do with tokenization.

NEW QUESTION: 114
In a cloud environment, encryption should be used for all the following, except:
Response:
A. Near-term storage of virtualized images
B. Profile formatting
C. Long-term storage of data
D. Secure sessions/VPN
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which of the following is the biggest concern or challenge with using encryption?
A. Dependence on keys
B. Cipher strength
C. Efficiency
D. Protocol standards
Answer: A (LEAVE A REPLY)
Explanation
No matter what kind of application, system, or hosting model used, encryption is 100 percent dependent on encryption keys. Properly securing the keys and the exchange of them is the biggest and most important challenge of encryption systems.

NEW QUESTION: 116
The BCDR plan/process should be written and documented in such a way that it can be used by _____.
Response:
A. Regulators

B. Essential BCDR team members
C. Someone with the requisite skills
D. Users
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Which of the following best describes SAML?
Response:
A. A standard for developing secure application management logistics
B. A standard for exchanging authentication and authorization data between security domains
C. A standard used for directory synchronization
D. A standard for exchanging usernames and passwords across devices
Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
Which of the following aspects of security is solely the responsibility of the cloud provider?
A. Regulatory compliance
B. Physical security
C. Operating system auditing
D. Personal security of developers
Answer: (SHOW ANSWER)
Regardless of the particular cloud service used, physical security of hardware and facilities is always the sole responsibility of the cloud provider. The cloud provider may release information about their physical security policies and procedures to ensure any particular requirements of potential customers will meet their regulatory obligations. Personal security of developers and regulatory compliance are always the responsibility of the cloud customer. Responsibility for operating systems, and the auditing of them, will differ based on the cloud service category used.

NEW QUESTION: 119
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)
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: 120
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
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: 121
Many different common threats exist against web-exposed services and applications. One attack involves attempting to leverage input fields to execute queries in a nested fashion that is unintended by the developers.
What type of attack is this?
A. Injection
B. Missing function-level access control
C. Cross-site scripting
D. Cross-site request forgery
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. This can trick an application into exposing data that is not intended or authorized to be exposed, or it can potentially allow an attacker to gain insight into configurations or security controls.
Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes.

NEW QUESTION: 122
Your boss has tasked your team with getting your legacy systems and applications connected with new cloud-based services that management has decided are crucial to customer service and offerings.
Which role would you be assuming under this directive?
A. Cloud service administrator
B. Cloud service user
C. Cloud service integrator
D. Cloud service business manager
Answer: (SHOW ANSWER)
Explanation
The cloud service integrator role is responsible for connecting and integrating existing services and applications with cloud-based services.A cloud service administrator is responsible for testing, monitoring, and securing cloud services, as well as providing usage reporting and dealing with service problems. The cloud service user is someone who consumes cloud services. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

NEW QUESTION: 123
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: 124

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/Reference:
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: 125
Which of the following terms is NOT a commonly used category of risk acceptance?
A. Moderate
B. Critical
C. Minimal
D. Accepted
Answer: (SHOW ANSWER)
Explanation
Explanation
Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

NEW QUESTION: 126
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: 127
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)
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: 128
Which ITIL component focuses on ensuring that system resources, processes, and personnel are properly allocated to meet SLA requirements?
A. Continuity management
B. Availability management
C. Configuration management
D. Problem management
Answer: B (LEAVE A REPLY)
Explanation
Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Configuration management tracks and maintains detailed information about all IT components within an organization. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION: 129
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)
Explanation/Reference:
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: 130
Which of the following concepts is NOT one of the core components to an encryption system architecture?
A. Software
B. Network
C. Keys
D. Data
Answer: B (LEAVE A REPLY)
Explanation
The network utilized is not one of the key components of an encryption system architecture. In fact, a network is not even required for encryption systems or the processing and protection of data. The data, software used for the encryption engine itself, and the keys used to implement the encryption are all core components of an encryption system architecture.

NEW QUESTION: 131
DLP can be combined with what other security technology to enhance data controls?
A. SIEM
B. Hypervisors
C. DRM
D. Kerberos
Answer: C (LEAVE A REPLY)
DLP can be combined with DRM to protect intellectual property; both are designed to deal with data that falls into special categories. SIEMs are used for monitoring event logs, not live data movement. Kerberos is an authentication mechanism. Hypervisors are used for virtualization.

NEW QUESTION: 132
Data labels could include all the following, except:
A. Distribution limitations
B. Multifactor authentication
C. Access restrictions
D. Confidentiality level
Answer: (SHOW ANSWER)

NEW QUESTION: 133

Which phase of the cloud data lifecycle also typically entails the process of data classification?
Response:
A. Archive
B. Create
C. Use
D. Store
Answer: B (LEAVE A REPLY)

NEW QUESTION: 134
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: 135
Which aspect of cloud computing serves as the biggest challenge to using DLP to protect data at rest?
A. Portability
B. Resource pooling
C. Interoperability
D. Reversibility
Answer: (SHOW ANSWER)
Resource pooling serves as the biggest challenge to using DLP solutions to protect data at rest because data is spread across large systems, which are also shared by many different clients. With the data always moving and being distributed, additional challenges for protection are created versus a physical and isolated storage system. Portability is the ability to easily move between different cloud providers, and interoperability is focused on

the ability to reuse components or services. Reversibility pertains to the ability of a cloud customer to easily and completely remove their data and services from a cloud provider.

NEW QUESTION: 136
Which is the lowest level of the CSA STAR program?
A. Attestation
B. Self-assessment
C. Hybridization
D. Continuous monitoring
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The lowest level is Level 1, which is self-assessment, Level 2 is an external third-party attestation, and Level 3 is a continuous-monitoring program. Hybridization does not exist as part of the CSA STAR program.

NEW QUESTION: 137
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)
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: 138

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: 139

What concept does the A represent within the DREAD model?

A. Affected users

B. Authorization

C. Authentication

D. Affinity

Answer: A (LEAVE A REPLY)

The concept of affected users measures the percentage of users who would be impacted by a successful exploit. Scoring ranges from 0, which would impact no users, to 10, which would impact all users. None of the other options provided is the correct term.

NEW QUESTION: 140

Which of the following roles is responsible for gathering metrics on cloud services and managing cloud deployments and the deployment processes?

A. Cloud service business manager

B. Cloud service operations manager

C. Cloud service manager

D. Cloud service deployment manager

Answer: (SHOW ANSWER)

The cloud service deployment manager is responsible for gathering metrics on cloud services, managing cloud deployments and the deployment process, and defining the environments and processes.

NEW QUESTION: 141

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
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: 142
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. Reconstruct your firewalls
B. Adjust the hypervisors
C. Survey your company's departments about the data under their control
D. Harden all your routers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
What is the only data format permitted with the SOAP API?
A. HTML
B. SAML
C. XSML
D. XML
Answer: D (LEAVE A REPLY)
Explanation
The SOAP protocol only supports the XML data format.

NEW QUESTION: 144
Although much of the attention given to data security is focused on keeping data private and only accessible by authorized individuals, of equal importance is the trustworthiness of the data.
Which concept encapsulates this?
A. Validity
B. Integrity
C. Accessibility
D. Confidentiality
Answer: B (LEAVE A REPLY)

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: 145
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: (SHOW ANSWER)
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: 146
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)
Data masking does not support authentication in any way. All the others are excellent use cases for data masking.

NEW QUESTION: 147
Which of the following security measures done at the network layer in a traditional data center are also applicable to a cloud environment?
A. Dedicated switches
B. Trust zones
C. Redundant network circuits
D. Direct connections
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:

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

NEW QUESTION: 148
What masking strategy involves the replacing of sensitive data at the time it is accessed and used as it flows between the data and application layers of a service?
A. Active
B. Static
C. Dynamic
D. Transactional
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Dynamic masking involves the live replacing of sensitive data fields during transactional use between the data and application layers of a service. Static masking involves creating a full data set with the sensitive data fields masked, but is not done during live transactions like dynamic masking. Active and transactional are offered as similar types of answers but are not types of masking.

NEW QUESTION: 149
What is the primary reason that makes resolving jurisdictional conflicts complicated?
A. Different technology standards
B. Costs
C. Language barriers
D. Lack of international authority
Answer: D (LEAVE A REPLY)
Explanation
With international operations, systems ultimately cross many jurisdictional boundaries, and many times, they conflict with each other. The major hurdle to overcome for an organization is the lack of an ultimate international authority to mediate such conflicts, with a likely result of legal efforts in each jurisdiction.

NEW QUESTION: 150
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: (SHOW ANSWER)

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: 151
Which of the following is the optimal temperature for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?
A. 69.8-86.0degF (21-30degC)
B. 64.4-80.6degF(18-27degC)
C. 51.8-66.2degF(11-19degC)
D. 44.6-60-8degF(7-16degC)
Answer: B (LEAVE A REPLY)
Explanation
The guidelines from ASHRAE establish 64.4-80.6degF (18-27degC) as the optimal temperature for a data center.

NEW QUESTION: 152
A process for _____ can aid in protecting against data disclosure due to lost devices.
Response:
A. User punishment
B. Credential revocation
C. Device tracking
D. Law enforcement notification

Answer: B (LEAVE A REPLY)

NEW QUESTION: 153
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/Reference:
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: 154
From a security perspective, automation of configuration aids in _____.
Response:
A. Increasing ease of use of the systems
B. Reducing need for administrative personnel
C. Reducing potential attack vectors
D. Enhancing performance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 155
Which of the following top security threats involves attempting to send invalid commands to an application in an attempt to get the application to execute the code?
A. Injection
B. Insecure direct object references
C. Cross-site scripting
D. Cross-site request forgery
Answer: (SHOW ANSWER)

NEW QUESTION: 156
A user signs on to a cloud-based social media platform. In another browser tab, the user finds an article worth posting to the social media platform. The user clicks on the platform's icon listed on the article's website, and the article is automatically posted to the user's account on the social media platform.
This is an example of what?
Response:
A. Insecure direct identifiers
B. Cross-site scripting

C. Identity federation
D. Single sign-on
Answer: C (LEAVE A REPLY)

NEW QUESTION: 157
When using a SaaS solution, what is the capability provided to the customer?
A. To use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
B. To use the consumer's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
C. To use the consumer's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
D. To use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Answer: D (LEAVE A REPLY)
Explanation
According to "The NIST Definition of Cloud Computing," in SaaS, "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

NEW QUESTION: 158

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

NEW QUESTION: 159
Which of the following is NOT a focus or consideration of an internal audit?
A. Certification
B. Design
C. Costs
D. Operational efficiency
Answer: (SHOW ANSWER)
Explanation
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: 160
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: 161
A truly airgapped machine selector will _____.
Response:
A. Terminate a connection before creating a new connection
B. Be made of composites and not metal
C. Have total Faraday properties
D. Not be portable

Answer: (SHOW ANSWER)

NEW QUESTION: 162
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
Which of these activities should you perform before deploying the tool?
Response:
A. Survey your company's departments about the data under their control
B. Harden all your routers
C. Adjust the hypervisors
D. Reconstruct your firewalls
Answer: A (LEAVE A REPLY)

NEW QUESTION: 163
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing.
According to the CSA, an organization that suffers a data breach might suffer all of the following negative effects except _____.
A. Loss of public perception/goodwill
B. Loss of market share
C. Cost of detection
D. Cost of compliance with notification laws
Answer: (SHOW ANSWER)

NEW QUESTION: 164
What controls the formatting and security settings of a volume storage system within a cloud environment?
A. Management plane
B. SAN host controller
C. Hypervisor
D. Operating system of the host
Answer: D (LEAVE A REPLY)
Explanation
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: 165
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)
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: 166
Above and beyond general regulations for data privacy and protection, certain types of data are subjected to more rigorous regulations and oversight.
Which of the following is not a regulatory framework for more sensitive or specialized data?
A. FIPS 140-2
B. FedRAMP
C. PCI DSS
D. HIPAA
Answer: (SHOW ANSWER)

The FIPS 140-2 standard pertains to the certification of cryptographic modules and is not a regulatory framework. The Payment Card Industry Data Security Standard (PCI DSS), the Federal Risk and Authorization Management Program (FedRAMP), and the Health Insurance Portability and Accountability Act (HIPAA) are all regulatory frameworks for sensitive or specialized data.

NEW QUESTION: 167
Which of the following is NOT a component of access control?
A. Accounting
B. Federation
C. Authorization
D. Authentication
Answer: (SHOW ANSWER)
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: 168
Which of the following roles is responsible for creating cloud components and the testing and validation of services?
A. Cloud auditor
B. Inter-cloud provider
C. Cloud service broker
D. Cloud service developer
Answer: D (LEAVE A REPLY)
Explanation
The cloud service developer is responsible for developing and creating cloud components and services, as well as for testing and validating services.

NEW QUESTION: 169
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: 170
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)
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: 171
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: 172
The goals of SIEM solution implementation include all of the following, except:
A. Dashboarding
B. Performance enhancement
C. Trend analysis
D. Centralization of log streams
Answer: B (LEAVE A REPLY)
Explanation
SIEM does not intend to provide any enhancement of performance; in fact, a SIEM solution may decrease performance because of additional overhead. All the rest are goals of SIEM implementations.

NEW QUESTION: 173
What are SOCI/SOCII/SOCIII?
A. Software development phases
B. Risk management frameworks
C. Access controls
D. Audit reports
Answer: D (LEAVE A REPLY)

NEW QUESTION: 174
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)
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: 175
Which European Union directive pertains to personal data privacy and an individual's control over their personal data?
A. 99/9/EC
B. 95/46/EC
C. 2000/1/EC
D. 2013/27001/EC
Answer: (SHOW ANSWER)
Directive 95/46/EC is titled "On the protection of individuals with regard to the processing of personal data and on the free movement of such data."

NEW QUESTION: 176
Humidity levels for a data center are a prime concern for maintaining electrical and computing resources properly as well as ensuring that conditions are optimal for top performance.
Which of the following is the optimal humidity level, as established by ASHRAE?
A. 20 to 40 percent relative humidity
B. 50 to 75 percent relative humidity
C. 40 to 60 percent relative humidity
D. 30 to 50 percent relative humidity
Answer: C (LEAVE A REPLY)
The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) recommends 40 to 60 percent relatively humidity for data centers. None of these options is the recommendation from ASHRAE.

NEW QUESTION: 177
What is the primary security mechanism used to protect SOAP and REST APIs?
A. XML firewalls
B. WAFs
C. Firewalls
D. Encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 178
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: 179
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: 180
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
What should you not expect the tool to address?
Response:
A. Sensitive data captured by screen shots
B. Sensitive data moved to external devices
C. Sensitive data in the contents of files sent via FTP
D. Sensitive data sent inadvertently in user emails
Answer: A (LEAVE A REPLY)

NEW QUESTION: 181
The destruction of a cloud customer's data can be required by all of the following except _____.
Response:

A. Statute
B. Contract
C. The cloud provider's policy
D. Regulation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 182
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: (SHOW ANSWER)
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: 183
Which of the following concepts is NOT one of the core components to an encryption system architecture?
A. Software
B. Network
C. Keys
D. Data
Answer: (SHOW ANSWER)
The network utilized is not one of the key components of an encryption system architecture. In fact, a network is not even required for encryption systems or the processing and protection of data. The data, software used for the encryption engine itself, and the keys used to implement the encryption are all core components of an encryption system architecture.

NEW QUESTION: 184
You are the IT director for a small contracting firm. Your company is considering migrating to a cloud production environment.
Which service model would best fit your needs if you wanted an option that reduced the chance of vendor lock-in but also did not require the highest degree of administration by your own personnel?
Response:
A. SaaS
B. TanstaafL
C. IaaS
D. PaaS
Answer: (SHOW ANSWER)

NEW QUESTION: 185
Which kind of SSAE report comes with a seal of approval from a certified auditor?
Response:
A. SOC 1
B. SOC 4
C. SOC 2
D. SOC 3
Answer: D (LEAVE A REPLY)

NEW QUESTION: 186
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)
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: 187
Egress monitoring solutions usually include a function that _____.
A. Resides on client machines
B. Uses biometrics to scan users
C. Inspects incoming packets

D. Uses stateful inspection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 188
Different certifications and standards take different approaches to data center design and operations. Although many traditional approaches use a tiered methodology, which of the following utilizes a macro-level approach to data center design?
A. IDCA
B. BICSI
C. Uptime Institute
D. NFPA
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The Infinity Paradigm of the International Data Center Authority (IDCA) takes a macro-level approach to data center design. The IDCA does not use a specific, focused approach on specific components to achieve tier status. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling.
The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers.

NEW QUESTION: 189
In order to ensure ongoing compliance with regulatory requirements, which phase of the cloud data lifecycle must be tested regularly?
A. Archive
B. Share
C. Store
D. Destroy
Answer: (SHOW ANSWER)
In order to ensure compliance with regulations, it is important for an organization to regularly test the restorability of archived data. As technologies change and older systems are deprecated, the risk rises for an organization to lose the ability to restore data from the format in which it is stored.
With the destroy, store, and share phases, the currently used technologies will be sufficient for an organization's needs in an ongoing basis, so the risk that is elevated with archived data is not present.

NEW QUESTION: 190
Within a federated identity system, which of the following would you be MOST likely to use for sending information for consumption by a relying party?

A. XML
B. HTML
C. WS-Federation
D. SAML
Answer: D (LEAVE A REPLY)
The Security Assertion Markup Language (SAML) is the most widely used method for encoding and sending attributes and other information from an identity provider to a relying party.WS- Federation, which is used by Active Directory Federation Services (ADFS), is the second most used method for sending information to a relying party, but it is not a better choice than SAML.
XML is similar to SAML in the way it encodes and labels data, but it does not have all of the required extensions that SAML does. HTML is not used within federated systems at all.

NEW QUESTION: 191
Which of these characteristics of a virtualized network adds risks to the cloud environment?
Response:
A. Scalability
B. Self-service
C. Pay-per-use
D. Redundancy
Answer: (SHOW ANSWER)