ISC.Premium.CCSP.by.VCEplus.512q

Number: CCSP VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 1.5

Exam Code: CCSP
Exam Name: Certified Cloud Security Professional (CCSP)
Certification Provider: ISC
Corresponding Certification: ISC-CCSP
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-CCSP/
Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in CCSP exam products and you get latest questions. We strive to deliver the best CCSP exam product for top grades in your first attempt.

Website: https://vceplus.com
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

QUESTION 1
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The cloud service developer is responsible for developing and creating cloud components and services, as well as for testing and validating services.

QUESTION 2
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Vendor documentation from the manufacturer of the physical hardware is the best source of best practices for securing the BIOS.

QUESTION 3
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The value of data itself has nothing to do with it being considered a part of contractual

QUESTION 4
Which of the following concepts refers to a cloud customer paying only for the resources and offerings they use within a cloud environment, and only for the duration that they are consuming them?

A. Consumable service
B. Measured service
C. Billable service
D. Metered service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Measured service is where cloud services are delivered and billed in a metered way, where the cloud customer only pays for those that they actually use, and for the duration of time that they use them.

QUESTION 5
Which of the following roles involves testing, monitoring, and securing cloud services for an organization?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 6
What is the only data format permitted with the SOAP API?

A. HTML
B. SAML
C. XSML
D. XML

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The SOAP protocol only supports the XML data format.

QUESTION 7
Which data formats are most commonly used with the REST API?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API, and are typically implemented with caching for increased scalability and performance.

QUESTION 8
Which of the following threat types involves an application that does not validate authorization for portions of itself after the initial checks?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 9
Which of the following roles involves overseeing billing, purchasing, and requesting audit reports for an organization within a cloud environment?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
The cloud service business manager is responsible for overseeing business and billing administration, purchasing cloud services, and requesting audit reports when necessary

QUESTION 10
What is the biggest concern with hosting a key management system outside of the cloud environment?

A. Confidentiality
B. Portability
C. Availability
D. Integrity

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 11
Which of the following approaches would NOT be considered sufficient to meet the requirements of secure data destruction within a cloud environment?

A. Cryptographic erasure
B. Zeroing
C. Overwriting
D. Deletion

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
Explanation

Deletion merely removes the pointers to data on a system; it does nothing to actually remove and sanitize the data. As such, the data remains in a recoverable state, and more secure methods are needed to ensure it has been destroyed and is not recoverable by another party.

QUESTION 12
Which of the following cloud aspects complicates eDiscovery?

A. Resource pooling
B. On-demand self-service
C. Multitenancy
D. Measured service

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 13
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 14
What is a serious complication an organization faces from the perspective of compliance with international operations?

A. Different certifications
B. Multiple jurisdictions
C. Different capabilities
D. Different operational procedures

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 15
Which networking concept in a cloud environment allows for network segregation and isolation of IP spaces?

A. PLAN
B. WAN
C. LAN
D. VLAN

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 16
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 17
Which of the following publishes the most commonly used standard for data center design in regard to tiers and topologies?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
The Uptime Institute publishes the most commonly used and widely known standard on data center tiers and topologies. It is based on a series of four tiers, with each progressive increase in number representing more stringent, reliable, and redundant systems for security, connectivity, fault tolerance, redundancy, and cooling.

QUESTION 18
What type of segregation and separation of resources is needed within a cloud environment for multitenancy purposes versus a traditional data center model?

A. Virtual
B. Security
C. Physical
D. Logical

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Cloud environments lack the ability to physically separate resources like a traditional data center can. To compensate, cloud computing logical segregation concepts are employed. These include VLANs, sandboxing, and the use of virtual network devices such as firewalls.

QUESTION 19
Which United States law is focused on data related to health records and privacy?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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.

QUESTION 20
What is used for local, physical access to hardware within a data center?

A. SSH
B. KVM
C. VPN
D. RDP

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 21
Within an Infrastructure as a Service model, which of the following would NOT be a measured service?

A. CPU
B. Storage
C. Number of users
D. Memory

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 22
Which of the following is NOT a criterion for data within the scope of eDiscovery?

A. Possession
B. Custody
C. Control
D. Archive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
eDiscovery pertains to information and data that is in the possession, control, and custody of an organization.

QUESTION 23
Which United States law is focused on accounting and financial practices of organizations?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 24
What type of masking strategy involves making a separate and distinct copy of data with masking in place?

A. Dynamic
B. Replication
C. Static
D. Duplication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
With static masking, a separate and distinct copy of the data set is created with masking in place. This is typically done through a script or other process that takes a standard data set, processes it to mask the appropriate and predefined fields, and then outputs the data set as a new one with the completed masking done.

QUESTION 25
Which of the following storage types is most closely associated with a database-type storage implementation?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
Explanation

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

QUESTION 26
Which of the following roles is responsible for overseeing customer relationships and the processing of financial transactions?

A. Cloud service manager
B. Cloud service deployment
C. Cloud service business manager
D. Cloud service operations manager

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The cloud service business manager is responsible for overseeing business plans and customer relationships as well as processing financial transactions.

QUESTION 27
Which protocol does the REST API depend on?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 28
Which United States program was designed to enable organizations to bridge the gap between privacy laws and requirements of the United States and the European Union?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Due to the lack of an adequate privacy law or protection at the federal level in the United States, European privacy regulations generally prohibit the exporting or sharing of PII from Europe with the United States. Participation in the Safe Harbor program is voluntary on behalf of an organization, but it does require them to conform to specific requirements and policies that mirror those from the EU. Thus, organizations can fulfill requirements for data sharing and export and possibly serve customers in the EU.

QUESTION 29
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 30
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 31
Which aspect of cloud computing will be most negatively impacted by vendor lock-in?

A. Elasticity
B. Reversibility
C. Interoperability

D. Portability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 32
Which of the following APIs are most commonly used within a cloud environment?

A. REST and SAML
B. SOAP and REST
C. REST and XML
D. XML and SAML

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
Explanation

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

QUESTION 33
Which of the following attempts to establish an international standard for eDiscovery processes and best practices?

A. ISO/IEC 31000
B. ISO/IEC 27050
C. ISO/IEC 19888
D. ISO/IEC 27001

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
ISO/IEC 27050 strives to establish an internationally accepted standard for eDiscovery processes and best practices. It encompasses all steps of the eDiscovery process: identification, preservation, collection, processing, review, analysis, and the final production of the requested data.

QUESTION 34
Which of the following roles is responsible for obtaining new customers and securing contracts and agreements?

A. Inter-cloud provider
B. Cloud service broker
C. Cloud auditor
D. Cloud service developer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
The cloud service broker is responsible for obtaining new customers, analyzing the marketplace, and securing contracts and agreements.

QUESTION 35
Which term relates to the application of scientific methods and practices to evidence?

A. Forensics
B. Methodical
C. Theoretical
D. Measured

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Forensics is the application of scientific and methodical processes to identify, collect, preserve, analyze, and summarize/report digital information and evidence.

QUESTION 36

Which of the following roles involves the provisioning and delivery of cloud services?

A. Cloud service deployment manager
B. Cloud service business manager
C. Cloud service manager
D. Cloud service operations manager

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The cloud service manager is responsible for the delivery of cloud services, the provisioning of cloud services, and the overall management of cloud services.

QUESTION 37
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 38
GAAPs are created and maintained by which organization?

A. ISO/IEC
B. AICPA
C. PCI Council
D. ISO

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
The AICPA is the organization responsible for generating and maintaining what are the Generally Accepted Accounting Practices in the United States.

QUESTION 39
Which of the following roles is responsible for preparing systems for the cloud, administering and monitoring services, and managing inventory and assets?

A. Cloud service business manager
B. Cloud service deployment manager
C. Cloud service operations manager
D. Cloud service manager

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 40
Which protocol allows a system to use block-level storage as if it was a SAN, but over TCP network traffic instead?

A. SATA
B. iSCSI
C. TLS
D. SCSI

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
iSCSI is a protocol that allows for the transmission and use of SCSI commands and features over a TCP-based network. iSCSI allows systems to use block-level storage that looks and behaves as a SAN would with physical servers, but to leverage the TCP network within a virtualized environment and cloud.

QUESTION 41
Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Popular services such as iCloud, Dropbox, and OneDrive are all publicly available and are open to any user for free, with possible add-on services offered for a cost.

QUESTION 42
Why does a Type 2 hypervisor typically offer less security control than a Type 1 hypervisor?

A. A Type 2 hypervisor runs on top of another operating system and is dependent on the security of the OS for its own security.
B. A Type 2 hypervisor allows users to directly perform some functions with their own access.
C. A Type 2 hypervisor is open source, so attackers can more easily find exploitable vulnerabilities with that access.
D. A Type 2 hypervisor is always exposed to the public Internet for federated identity access.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 43
Which is the appropriate phase of the cloud data lifecycle for determining the data's classification?

A. Create
B. Use
C. Share
D. Store

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Any time data is created, modified, or imported, the classification needs to be evaluated and set from the earliest phase to ensure security is always properly maintained for the duration of its lifecycle.

QUESTION 44
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)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
The guidelines from ASHRAE establish 64.4-80.6degF (18-27degC) as the optimal temperature for a data center.

QUESTION 45
Which of the following is not a risk management framework?

A. COBIT
B. Hex GBL
C. ISO 31000:2009
D. NIST SP 800-37

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe. The rest are not.

QUESTION 46
Which of the following threat types involves the sending of untrusted data to a user's browser to be executed with their own credentials and access?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or where the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with the user's own access and permissions, allowing an attacker to redirect their web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access.

QUESTION 47
How is an object stored within an object storage system?

A. Key value
B. Database
C. LDAP
D. Tree structure

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Object storage uses a flat structure with key values to store and access objects.

QUESTION 48
Which of the following is NOT a regulatory system from the United States federal government?

A. PCI DSS
B. FISMA
C. SOX
D. HIPAA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 49
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 50
Which United States law is focused on PII as it relates to the financial industry?

A. HIPAA
B. SOX
C. Safe Harbor

D. GLBA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The GLBA, as it is commonly called based on the lead sponsors and authors of the act, is officially known as "The Financial Modernization Act of 1999." It is specifically focused on PII as it relates to financial institutions. There are three specific components of it, covering various areas and use, on top of a general requirement that all financial institutions must provide all users and customers with a written copy of their privacy policies and practices, including with whom and for what reasons their information may be shared with other entities.

QUESTION 51
Which of the following threat types can occur when encryption is not properly applied or insecure transport mechanisms are used?

A. Security misconfiguration
B. Insecure direct object references
C. Sensitive data exposure
D. Unvalidated redirects and forwards

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 52
What is the best approach for dealing with services or utilities that are installed on a system but not needed to perform their desired function?

A. Remove
B. Monitor
C. Disable

D. Stop

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 53
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 54
What are the two protocols that TLS uses?

A. Handshake and record
B. Transport and initiate
C. Handshake and transport
D. Record and transmit

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
TLS uses the handshake protocol to establish and negotiate the TLS connection, and it uses the record protocol for the secure transmission of data.

QUESTION 55
Which type of cloud model typically presents the most challenges to a cloud customer during the "destroy" phase of the cloud data lifecycle?

A. IaaS
B. DaaS
C. SaaS
D. PaaS

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 56
Which of the following may unilaterally deem a cloud hosting model inappropriate for a system or application?

A. Multitenancy
B. Certification
C. Regulation
D. Virtualization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Some regulations may require specific security controls or certifications be used for hosting certain types of data or functions, and in some circumstances they may be requirements that are unable to be met by any cloud provider.

QUESTION 57
Which of the following is considered an internal redundancy for a data center?

A. Power distribution units
B. Network circuits
C. Power substations
D. Generators

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Power distribution units are internal to a data center and supply power to internal components such as racks, appliances, and cooling systems. As such, they are considered an internal redundancy.

QUESTION 58
Which of the following represents a control on the maximum amount of resources that a single customer, virtual machine, or application can consume within a cloud environment?

A. Share
B. Reservation
C. Provision
D. Limit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Limits are put in place to enforce a maximum on the amount of memory or processing a cloud customer can use. This can be done either on a virtual machine or as a comprehensive whole for a customer, and is meant to ensure that enormous cloud resources cannot be allocated or consumed by a single host or customer to the detriment of other hosts and customers.

QUESTION 59
Which of the following roles is responsible for peering with other cloud services and providers?

A. Cloud auditor
B. Inter-cloud provider
C. Cloud service broker

D. Cloud service developer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated services.

QUESTION 60
Which of the following does NOT relate to the hiding of sensitive data from data sets?

A. Obfuscation
B. Federation
C. Masking
D. Anonymization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Federation pertains to authenticating systems between different organizations.

QUESTION 61
Which of the following are the storage types associated with IaaS?

A. Volume and object
B. Volume and label
C. Volume and container
D. Object and target

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which technology can be useful during the "share" phase of the cloud data lifecycle to continue to protect data as it leaves the original system and security controls?

A. IPS
B. WAF
C. DLP
D. IDS

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 63
Which of the following storage types is most closely associated with a traditional file system and tree structure?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 64
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
Explanation

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

QUESTION 65
Which type of audit report does many cloud providers use to instill confidence in their policies, practices, and procedures to current and potential customers?

A. SAS-70
B. SOC 2
C. SOC 1
D. SOX

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
One approach that many cloud providers opt to take is to undergo a SOC 2 audit and make the report available to cloud customers and potential cloud customers as a way of providing security confidence without having to open their systems or sensitive information to the masses.

QUESTION 66
Which of the following statements accurately describes VLANs?

A. They are not restricted to the same data center or the same racks.

B. They are not restricted to the name rack but restricted to the same data center.
C. They are restricted to the same racks and data centers.
D. They are not restricted to the same rack but restricted to same switches.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A virtual area network (VLAN) can span any networks within a data center, or it can span across different physical locations and data centers.

QUESTION 67
What must be secured on physical hardware to prevent unauthorized access to systems?

A. BIOS
B. SSH
C. RDP
D. ALOM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
BIOS is the firmware that governs the physical initiation and boot up of a piece of hardware. If it is compromised, an attacker could have access to hosted systems and make configurations changes to expose or disable some security elements on the system.

QUESTION 68
What type of PII is regulated based on the type of application or per the conditions of the specific hosting agreement?

A. Specific
B. Contractual
C. regulated
D. Jurisdictional

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Contractual PII has specific requirements for the handling of sensitive and personal information, as defined at a contractual level. These specific requirements will typically document the required handling procedures and policies to deal with PII. They may be in specific security controls and configurations, required policies or procedures, or limitations on who may gain authorized access to data and systems.

QUESTION 69
Which of the following security technologies is commonly used to give administrators access into trust zones within an environment?

A. VPN
B. WAF
C. IPSec
D. HTTPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Virtual private networks (VPNs) are commonly used to allow access into trust zones. Via a VPN, access can be controlled and logged and only allowed through secure channels by authorized users. It also adds an additional layer of encryption and protection to communications.

QUESTION 70
Which concept BEST describes the capability for a cloud environment to automatically scale a system or application, based on its current resource demands?

A. On-demand self-service
B. Resource pooling
C. Measured service
D. Rapid elasticity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Rapid elasticity allows a cloud environment to automatically add or remove resources to or from a system or application based on its current demands. Whereas a traditional data center model would require standby hardware and substantial effort to add resources in response to load increases, a cloud environment can easily and rapidly expand to meet resources demands, so long as the application is properly implemented for it.

QUESTION 71
If you're using iSCSI in a cloud environment, what must come from an external protocol or application?

A. Kerberos support
B. CHAP support
C. Authentication
D. Encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
iSCSI does not natively support encryption, so another technology such as IPsec must be used to encrypt communications.

QUESTION 72
Which of the following pertains to a macro level approach to data center design rather than the traditional tiered approach to data centers?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 73
What does the REST API support that SOAP does NOT support?

A. Caching
B. Encryption

C. Acceleration
D. Redundancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
The SOAP protocol does not support caching, whereas the REST API does.

QUESTION 74
Why does a Type 1 hypervisor typically offer tighter security controls than a Type 2 hypervisor?

A. A Type 1 hypervisor also controls patching of its hosted virtual machines ensure they are always secure.
B. A Type 1 hypervisor is tied directly to the bare metal and only runs with code necessary to perform its specific mission.
C. A Type 1 hypervisor performs hardware-level encryption for tighter security and efficiency.
D. A Type 1 hypervisor only hosts virtual machines with the same operating systems as the hypervisor.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 75
Which of the following are the storage types associated with PaaS?

A. Structured and freeform
B. Volume and object
C. Structured and unstructured
D. Database and file system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following threat types can occur when baselines are not appropriately applied or unauthorized changes are made?

A. Insecure direct object references
B. Unvalidated redirects and forwards
C. Security misconfiguration
D. Sensitive data exposure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner. This can be caused from a shortcoming in security baselines or configurations, unauthorized changes to system configurations, or a failure to patch and upgrade systems as the vendor releases security patches.

QUESTION 77
What is the data encapsulation used with the SOAP protocol referred to?

A. Packet
B. Envelope
C. Payload
D. Object

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Simple Object Access Protocol (SOAP) encapsulates its information in what is known as a SOAP envelope and then leverages common communications protocols for transmission.

QUESTION 78
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
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.

QUESTION 79
Which publication from the United States National Institute of Standards and Technology pertains to defining cloud concepts and definitions for the various core components of cloud computing?

A. SP 800-153
B. SP 800-145
C. SP 800-53
D. SP 800-40

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
NIST Special Publications 800-145 is titled "The NIST Definition of Cloud Computing" and contains definitions and explanations of core cloud concepts and components.

QUESTION 80
What is the biggest negative to leasing space in a data center versus building or maintain your own?

A. Costs
B. Control
C. Certification
D. Regulation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
When leasing space in a data center, an organization will give up a large degree of control as to how it is built and maintained, and instead must conform to the policies and procedures of the owners and operators of the data center.

QUESTION 81
Which aspect of archiving must be tested regularly for the duration of retention requirements?

A. Availability
B. Recoverability
C. Auditability
D. Portability

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 82
Which of the following represents a minimum guaranteed resource within a cloud environment for the cloud customer?

A. Reservation
B. Share

C. Limit
D. Provision

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 83
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 84
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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 85
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 86
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 87
Which technology is NOT commonly used for security with data in transit?

A. DNSSEC
B. IPsec
C. VPN
D. HTTPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
DNSSEC relates to the integrity of DNS resolutions and the prevention of spoofing or redirection, and does not pertain to the actual security of transmissions or the protection of data.

QUESTION 88
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 89
Which of the following is considered an external redundancy for a data center?

A. Power feeds to rack
B. Generators
C. Power distribution units
D. Storage systems

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Generators are considered an external redundancy to a data center. Power distribution units (PDUs), storage systems, and power feeds to racks are all internal to a data center, and as such they are considered internal redundancies.

QUESTION 90
Which of the following is the optimal humidity level for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?

A. 30-50 percent relative humidity
B. 50-75 percent relative humidity
C. 20-40 percent relative humidity
D. 40-60 percent relative humidity

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 91
What is the first stage of the cloud data lifecycle where security controls can be implemented?

A. Use
B. Store
C. Share
D. Create

Correct Answer: B

Section: (none)
Explanation

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

QUESTION 92
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
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.

QUESTION 93
What does SDN stand for within a cloud environment?

A. Software-dynamic networking
B. Software-defined networking
C. Software-dependent networking
D. System-dynamic nodes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Software-defined networking separates the administration of network filtering and network forwarding to allow for distributed administration.

QUESTION 94
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 95
Which of the following would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?

A. Resource pooling
B. Virtualization
C. Multitenancy
D. Regulation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers, and especially within a public cloud model, it is not possible or practical for a cloud provider to alter their services for specific customer demands.

QUESTION 96
Which of the following pertains to fire safety standards within a data center, specifically with their enormous electrical consumption?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 97
Which of the following roles involves the connection and integration of existing systems and services to a cloud environment?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The cloud service integrator is the official role that involves connecting and integrating existing systems and services with a cloud environment. This may involve moving services into a cloud environment, or connecting to external cloud services and capabilities from traditional data center-hosted services.

QUESTION 98
Which technique involves replacing values within a specific data field to protect sensitive data?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 99
What expectation of data custodians is made much more challenging by a cloud implementation, especially with PaaS or SaaS?

A. Data classification
B. Knowledge of systems
C. Access to data
D. Encryption requirements

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
Explanation

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

QUESTION 100
What type of PII is controlled based on laws and carries legal penalties for noncompliance with requirements?

A. Contractual
B. Regulated
C. Specific
D. Jurisdictional

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Regulated PII involves those requirements put forth by specific laws or regulations, and unlike contractual PII, where a violation can lead to contractual penalties, a violation of regulated PII can lead to fines or even criminal charges in some jurisdictions. PII regulations can depend on either the jurisdiction that applies to the hosting location or application or specific legislation based on the industry or type of data used.

QUESTION 101
Which if the following is NOT one of the three components of a federated identity system transaction?

A. Relying party
B. Identity provider
C. User
D. Proxy relay

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Which value refers to the amount of time it takes to recover operations in a BCDR situation to meet management's objectives?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 103
Which of the cloud deployment models requires the cloud customer to be part of a specific group or organization in order to host cloud services within it?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 104
What provides the information to an application to make decisions about the authorization level appropriate when granting access?

A. User
B. Relying party
C. Federation
D. Identity Provider

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 105
What is a standard configuration and policy set that is applied to systems and virtual machines called?

A. Standardization
B. Baseline
C. Hardening

D. Redline

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 106
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 107
Which of the cloud cross-cutting aspects relates to the ability to easily move services and applications between different cloud providers?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 108
Which type of audit report is considered a "restricted use" report for its intended audience?

A. SAS-70
B. SSAE-16
C. SOC Type 1
D. SOC Type 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
SOC Type 1 reports are considered "restricted use" reports. They are intended for management and stakeholders of an organization, clients of the service organization, and auditors of the organization. They are not intended for release beyond those audiences.

QUESTION 109
What is the concept of segregating information or processes, within the same system or application, for security reasons?

A. fencing
B. Sandboxing
C. Cellblocking
D. Pooling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Sandboxing involves segregating and isolating information or processes from others within the same system or application, typically for security concerns. This is generally used for data isolation (for example, keeping different communities and populations of users isolated from other similar data).

QUESTION 110
The European Union passed the first major regulation declaring data privacy to be a human right. In what year did it go into effect?

A. 2010
B. 2000
C. 1995
D. 1990

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Adopted in 1995, Directive 95/46 EC establishes strong data protection and policy requirements, including the declaring of data privacy to be a human right. It establishes that an individual has the right to be notified when their personal data is being access or processed, that it only will ever be accessed for legitimate purposes, and that data will only be accessed to the exact extent it needs to be for the particular process or request.

QUESTION 111
Which of the following is NOT a key area for performance monitoring as far as an SLA is concerned?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 112
Which of the following is the MOST important requirement and guidance for testing during an audit?

A. Stakeholders
B. Shareholders
C. Management
D. Regulations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
During any audit, regulations are the most important factor and guidelines for what must be tested. Although the requirements from management, stakeholders, and shareholders are also important, regulations are not negotiable and pose the biggest risk to any organization for compliance failure.

QUESTION 113
Which value refers to the amount of data an organization would need to recover in the event of a BCDR situation in order to reach an acceptable level of operations?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 114
What must SOAP rely on for security?

A. Encryption
B. Tokenization
C. TLS
D. SSL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

QUESTION 115
Which of the following is a commonly used tool for maintaining system configurations?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 116
What type of data does data rights management (DRM) protect?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 117
Which type of testing uses the same strategies and toolsets that hackers would use?

A. Penetration
B. Dynamic

C. Static
D. Malicious

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 118
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 119
Which of the following is NOT a focus or consideration of an internal audit?

A. Certification
B. Design
C. Costs
D. Operational efficiency

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 120
Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?

A. Infrastructure
B. Platform
C. Application
D. Data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Regardless of which cloud-hosting model is used, the cloud customer always has sole responsibility for the data and its security.

QUESTION 121
What process is used within a clustered system to provide high availability and load balancing?

A. Dynamic balancing
B. Dynamic clustering
C. Dynamic optimization
D. Dynamic resource scheduling

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 122
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 123
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 124
What changes are necessary to application code in order to implement DNSSEC?

A. Adding encryption modules
B. Implementing certificate validations
C. Additional DNS lookups
D. No changes are needed.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 125
Which type of controls are the SOC Type 1 reports specifically focused on?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 126
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 127
Which of the following is NOT a domain of the Cloud Controls Matrix (CCM)?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Budgetary and cost controls is not one of the domains outlined in the CCM.

QUESTION 128
Which security concept, if implemented correctly, will protect the data on a system, even if a malicious actor gains access to the actual system?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 129
Which of the following is the sole responsibility of the cloud provider, regardless of which cloud model is used?

A. Platform
B. Data
C. Physical environment

D. Infrastructure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Regardless of which cloud-hosting model is used, the cloud provider always has sole responsibility for the physical environment.

QUESTION 130
Which of the following is NOT a factor that is part of a firewall configuration?

A. Encryption
B. Port
C. Protocol
D. Source IP

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 131
Which of the cloud deployment models involves spanning multiple cloud environments or a mix of cloud hosting models?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Section: (none)
Explanation

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

QUESTION 132
Which of the following is NOT one of five principles of SOC Type 2 audits?

A. Privacy
B. Processing integrity
C. Financial
D. Security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The SOC Type 2 audits include five principles: security, privacy, processing integrity, availability, and confidentiality.

QUESTION 133
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 134
What concept does the "T" represent in the STRIDE threat model?

A. TLS
B. Testing
C. Tampering with data
D. Transport

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation
Any application that sends data to the user will face the potential that the user could manipulate or alter the data, whether it resides in cookies, GET or POST commands, or headers, or manipulates client-side validations. If the user receives data from the application, it is crucial that the application validate and verify any data that is received back from the user.

QUESTION 135
Which of the following would be a reason to undertake a BCDR test?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 136
What is the biggest challenge to data discovery in a cloud environment?

A. Format
B. Ownership
C. Location

D. Multitenancy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
With the distributed nature of cloud environments, the foremost challenge for data discovery is awareness of the location of data and keeping track of it during the constant motion of cloud storage systems.

QUESTION 137
Which crucial aspect of cloud computing can be most threatened by insecure APIs?

A. Automation
B. Redundancy
C. Resource pooling
D. Elasticity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Cloud environments depend heavily on API calls for management and automation. Any vulnerability with the APIs can cause significant risk and exposure to all tenants of the cloud environment.

QUESTION 138
Which of the following should NOT be part of the requirement analysis phase of the software development lifecycle?

A. Functionality
B. Programming languages
C. Software platform
D. Security requirements

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 139
Which of the cloud cross-cutting aspects relates to the assigning of jobs, tasks, and roles, as well as to ensuring they are successful and properly performed?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 140
Which regulatory system pertains to the protection of healthcare data?

A. HIPAA
B. HAS
C. HITECH
D. HFCA

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 141
Which aspect of cloud computing makes it very difficult to perform repeat audits over time to track changes and compliance?

A. Virtualization

B. Multitenancy
C. Resource pooling
D. Dynamic optimization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Cloud environments will regularly change virtual machines as patching and versions are changed. Unlike a physical environment, there is little continuity from one period of time to another. It is very unlikely that the same virtual machines would be in use during a repeat audit.

QUESTION 142
Which security concept would business continuity and disaster recovery fall under?

A. Confidentiality
B. Availability
C. Fault tolerance
D. Integrity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 143
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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 144
Which of the cloud cross-cutting aspects relates to the ability for a cloud customer to easily remove their applications and data from a cloud environment?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 145
Which of the following is NOT a function performed by the record protocol of TLS?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 146
What concept does the "R" represent with the DREAD model?

A. Reproducibility
B. Repudiation
C. Risk
D. Residual

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reproducibility is the measure of how easy it is to reproduce and successful use an exploit. Scoring within the DREAD model ranges from 0, signifying a nearly impossibly exploit, up to 10, which signifies something that anyone from a simple function call could exploit, such as a URL.

QUESTION 147
The SOC Type 2 reports are divided into five principles.
Which of the five principles must also be included when auditing any of the other four principles?

A. Confidentiality
B. Privacy
C. Security
D. Availability

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 148
How many additional DNS queries are needed when DNSSEC integrity checks are added?

A. Three
B. Zero

C. One
D. Two

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
DNSSEC does not require any additional DNS queries to be performed. The DNSSEC integrity checks and validations are all performed as part of the single DNS lookup resolution.

QUESTION 149
Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?

A. Platform
B. Infrastructure
C. Governance
D. Application

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Regardless of which cloud-hosting model is used, the cloud customer always has sole responsibility for the governance of systems and data.

QUESTION 150
Which of the following service categories entails the least amount of support needed on the part of the cloud customer?

A. SaaS
B. IaaS
C. DaaS
D. PaaS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
With SaaS providing a fully functioning application that is managed and maintained by the cloud provider, cloud customers incur the least amount of support responsibilities themselves of any service category.

QUESTION 151
Which of the following would NOT be a reason to activate a BCDR strategy?

A. Staffing loss
B. Terrorism attack
C. Utility disruptions
D. Natural disaster

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 152
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 153

Which of the cloud cross-cutting aspects relates to the ability to reuse or move components of an application or service?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 154
Which of the following is a restriction that can be enforced by information rights management (IRM) that is not possible for traditional file system controls?

A. Delete
B. Modify
C. Read
D. Print

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 155
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 156
What type of security threat is DNSSEC designed to prevent?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
Explanation

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

QUESTION 157
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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."

QUESTION 158
Which of the cloud cross-cutting aspects relates to the requirements placed on a system or application by law, policy, or requirements from standards?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Regulatory requirements are those imposed upon businesses and their operations either by law, regulation, policy, or standards and guidelines. These requirements are specific either to the locality in which the company or application is based or to the specific nature of the data and transactions conducted.

QUESTION 159
Which data point that auditors always desire is very difficult to provide within a cloud environment?

A. Access policy
B. Systems architecture
C. Baselines
D. Privacy statement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Cloud environments are constantly changing and often span multiple physical locations. A cloud customer is also very unlikely to have knowledge and insight into the underlying systems architecture in a cloud environment. Both of these realities make it very difficult, if not impossible, for an organization to provide a comprehensive systems design document.

QUESTION 160
What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?

A. Proxy
B. Bastion
C. Honeypot
D. WAF

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
A bastion host is a server that is fully exposed to the public Internet, but is extremely hardened to prevent attacks and is usually dedicated for a specific application or usage; it is not something that will serve multiple purposes. This singular focus allows for much more stringent security hardening and monitoring.

QUESTION 161
Which security concept is focused on the trustworthiness of data?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Integrity is focused on the trustworthiness of data as well as the prevention of unauthorized modification or tampering of it. A prime consideration for maintaining integrity is an emphasis on the change management and configuration management aspects of operations, so that all modifications are predictable, tracked, logged, and verified, whether they are performed by actual human users or systems processes and scripts.

QUESTION 162
Which OSI layer does IPsec operate at?

A. Network
B. transport
C. Application
D. Presentation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A major difference between IPsec and other protocols such as TLS is that IPsec operates at the Internet network layer rather than the application layer, allowing for complete end-to-end encryption of all communications and traffic.

QUESTION 163
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
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.

QUESTION 164
Which of the following service capabilities gives the cloud customer the most control over resources and configurations?

A. Desktop
B. Platform
C. Infrastructure
D. Software

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 165
What concept does the "I" represent with the STRIDE threat model?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 166
At which stage of the BCDR plan creation phase should security be included in discussions?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Security should be included in discussions from the very first phase when defining the scope. Adding security later is likely to incur additional costs in time and

money, or will result in an incomplete or inadequate plan.

QUESTION 167
Which approach is typically the most efficient method to use for data discovery?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 168
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 169
Which audit type has been largely replaced by newer approaches since 2011?

A. SOC Type 1
B. SSAE-16

C. SAS-70
D. SOC Type 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
SAS-70 reports were replaced in 2011 with the SSAE-16 reports throughout the industry.

QUESTION 170
Which of the following can be useful for protecting cloud customers from a denial-of-service (DoS) attack against another customer hosted in the same cloud?

A. Reservations
B. Measured service
C. Limits
D. Shares

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reservations ensure that a minimum level of resources will always be available to a cloud customer for them to start and operate their services. In the event of a DoS attack against one customer, they can guarantee that the other customers will still be able to operate.

QUESTION 171
Which of the following service capabilities gives the cloud customer the least amount of control over configurations and deployments?

A. Platform
B. Infrastructure
C. Software
D. Desktop

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The software service capability gives the cloud customer a fully established application, where only minimal user configuration options are allowed.

QUESTION 172
What does the "SOC" acronym refer to with audit reports?

A. Service Origin Confidentiality
B. System Organization Confidentiality
C. Service Organizational Control
D. System Organization Control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
What does the REST API use to protect data transmissions?

A. NetBIOS
B. VPN
C. Encapsulation
D. TLS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Representational State Transfer (REST) uses TLS for communication over secured channels. Although REST also supports SSL, at this point SSL has been phased out due to vulnerabilities and has been replaced by TLS.

QUESTION 174
What strategy involves replacing sensitive data with opaque values, usually with a means of mapping it back to the original value?

A. Masking

B. Anonymization
C. Tokenization
D. Obfuscation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
Explanation

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

QUESTION 175
With software-defined networking, what aspect of networking is abstracted from the forwarding of traffic?

A. Routing
B. Session
C. Filtering
D. Firewalling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
With software-defined networking (SDN), the filtering of network traffic is separated from the forwarding of network traffic so that it can be independently administered.

QUESTION 176
Which of the following does NOT fall under the "IT" aspect of quality of service (QoS)?

A. Applications
B. Key performance indicators (KPIs)

C. Services
D. Security

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
KPIs fall under the "business" aspect of QoS, along with monitoring and measuring of events and business processes. Services, security, and applications are all core components and concepts of the "IT" aspect of QoS.

QUESTION 177
What does dynamic application security testing (DAST) NOT entail?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 178
Where is an XML firewall most commonly deployed in the environment?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 179
What type of masking strategy involves replacing data on a system while it passes between the data and application layers?

A. Dynamic
B. Static
C. Replication
D. Duplication

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 180
Which of the following is a widely used tool for code development, branching, and collaboration?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 181
Which aspect of security is DNSSEC designed to ensure?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 182
Which process serves to prove the identity and credentials of a user requesting access to an application or data?

A. Repudiation
B. Authentication
C. Identification
D. Authorization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Authentication is the process of proving whether the identity presented by a user is true and valid. This can be done through common mechanisms such as user ID and password combinations or with more secure methods such as multifactor authentication.

QUESTION 183
Who would be responsible for implementing IPsec to secure communications for an application?

A. Developers
B. Systems staff
C. Auditors
D. Cloud customer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Because IPsec is implemented at the system or network level, it is the responsibility of the systems staff. IPsec removes the responsibility from developers, whereas other technologies such as TLS would be implemented by developers.

QUESTION 184
What is the minimum regularity for testing a BCDR plan to meet best practices?

A. Once year
B. Once a month
C. Every six months
D. When the budget allows it

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 185
Other than cost savings realized due to measured service, what is another facet of cloud computing that will typically save substantial costs in time and money for an organization in the event of a disaster?

A. Broad network access
B. Interoperability
C. Resource pooling
D. Portability

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
With a typical BCDR solution, an organization would need some number of staff to quickly travel to the location of the BCDR site to configure systems and

applications for recovery. With a cloud environment, everything is done over broad network access, with no need (or even possibility) to travel to a remote site at any time.

QUESTION 186
Which of the following is NOT part of a retention policy?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 187
Which aspect of cloud computing would make the use of a cloud the most attractive as a BCDR solution?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 188
Which of the cloud deployment models offers the easiest initial setup and access for the cloud customer?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Because the public cloud model is available to everyone, in most instances all a customer will need to do to gain access is set up an account and provide a credit card number through the service's web portal. No additional contract negotiations, agreements, or specific group memberships are typically needed to get started.

QUESTION 189
Which of the following is NOT something that an HIDS will monitor?

A. Configurations
B. User logins
C. Critical system files
D. Network traffic

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 190
Which of the following technologies is used to monitor network traffic and notify if any potential threats or attacks are noticed?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
An intrusion detection system (IDS) is designed to analyze network packets, compare their contents or characteristics against a set of configurations or signatures, and alert personnel if anything is detected that could constitute a threat or is otherwise designated for alerting.

QUESTION 191
What concept does the "A" represent in the DREAD model?

A. Affected users
B. Authentication
C. Affinity
D. Authorization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Affected users refers to the percentage of users who would be impacted by a successful exploit. Scoring ranges from 0, which means no users are impacted, to 10, which means all users are impacted.

QUESTION 192
Which attribute of data poses the biggest challenge for data discovery?

A. Labels
B. Quality
C. Volume
D. Format

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 193
What does static application security testing (SAST) offer as a tool to the testers?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Static application security testing (SAST) is conducted with knowledge of the system, including source code, and is done against offline systems.

QUESTION 194
Which of the following service capabilities gives the cloud customer an established and maintained framework to deploy code and applications?

A. Software
B. Desktop
C. Platform
D. Infrastructure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The platform service capability provides programming languages and libraries from the cloud provider, where the customer can deploy their own code and applications into a managed and controlled framework.

QUESTION 195
What process is used within a cloud environment to maintain resource balancing and ensure that resources are available where and when needed?

A. Dynamic clustering
B. Dynamic balancing
C. Dynamic resource scheduling
D. Dynamic optimization

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 196
Which value refers to the percentage of production level restoration needed to meet BCDR objectives?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 197
Over time, what is a primary concern for data archiving?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Over time, maintaining the ability to restore and read archives is a primary concern for data archiving. As technologies change and new systems are brought in,

it is imperative for an organization to ensure they are still able to restore and access archives for the duration of the required retention period.

QUESTION 198
What is an often overlooked concept that is essential to protecting the confidentiality of data?

A. Strong password
B. Training
C. Security controls
D. Policies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
While the main focus of confidentiality revolves around technological requirements or particular security methods, an important and often overlooked aspect of safeguarding data confidentiality is appropriate and comprehensive training for those with access to it. Training should be focused on the safe handling of sensitive information overall, including best practices for network activities as well as physical security of the devices or workstations used to access the application.

QUESTION 199
Which of the cloud deployment models offers the most control and input to the cloud customer as to how the overall cloud environment is implemented and configured?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 200

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 201
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 202
One of the main components of system audits is the ability to track changes over time and to match these changes with continued compliance and internal processes.

Which aspect of cloud computing makes this particular component more challenging than in a traditional data center?

A. Portability
B. Virtualization
C. Elasticity
D. Resource pooling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
Explanation

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

QUESTION 203
In the wake of many scandals with major corporations involving fraud and the deception of investors and regulators, which of the following laws was passed to govern accounting and financial records and disclosures?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and accounting errors.The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy. The

Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Safe Harbor program was designed by the US government as a way for American companies to comply with European Union privacy laws.

QUESTION 204
Which one of the following threat types to applications and services involves the sending of requests that are invalid and manipulated through a user's client to execute commands on the application under the user's own credentials?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 205
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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.

QUESTION 206
You just hired an outside developer to modernize some applications with new web services and functionality. In order to implement a comprehensive test platform for validation, the developer needs a data set that resembles a production data set in both size and composition.
In order to accomplish this, what type of masking would you use?

A. Development
B. Replicated
C. Static
D. Dynamic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Static masking takes a data set and produces a copy of it, but with sensitive data fields masked. This allows for a full data set from production for testing purposes, but without any sensitive data. Dynamic masking works with a live system and is not used to produce a distinct copy. The terms "replicated" and "development" are not types of masking.

QUESTION 207
In order to prevent cloud customers from potentially consuming enormous amounts of resources within a cloud environment and thus having a negative impact on other customers, what concept is commonly used by a cloud provider?

A. Limit
B. Cap
C. Throttle
D. Reservation

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 208
Where is a DLP solution generally installed when utilized for monitoring data at rest?

A. Network firewall
B. Host system
C. Application server
D. Database server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
To monitor data at rest appropriately, the DLP solution would be installed on the host system where the data resides. A database server, in some situations, may be an appropriate answer, but the host system is the best answer because a database server is only one example of where data could reside. An application server processes data and typically sits between the data and presentation zones, and as such, does not store data at rest. A network firewall would be more appropriate for data in transit because it is not a place where data would reside.

QUESTION 209
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Regardless of the particular cloud service used, physical security of hardware and facilities is always the sole responsibility of the cloud provider. The cloud