ISC.CCSP.by.Atony.221q

Number: CCSP
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: CCSP
Exam Name: Certified Cloud Security Professional (CCSP)

Exam A

QUESTION 1
Which cloud storage type requires special consideration on the part of the cloud customer to ensure they do not program themselves into a vendor lock-in situation?

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

Correct Answer: D
Section:
Explanation:
Structured storage is designed, maintained, and implemented by a cloud service provider as part of a PaaS offering. It is specific to that cloud provider and the way they have opted to implement systems, so special care is required to ensure that applications are not designed in a way that will lock the cloud customer into a specific cloud provider with that dependency. Unstructured storage for auxiliary files would not lock a customer into a specific provider. With volume and object storage, because the cloud customer maintains their own systems with IaaS, moving and replicating to a different cloud provider would be very easy.

QUESTION 2
Which cloud deployment model would be ideal for a group of universities looking to work together, where each university can gain benefits according to its specific needs?

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

Correct Answer: D
Section:
Explanation:
A community cloud is owned and maintained by similar organizations working toward a common goal. In this case, the universities would all have very similar needs and calendar requirements, and they would not be financial competitors of each other. Therefore, this would be an ideal group for working together within a community cloud. A public cloud model would not work in this scenario because it is designed to serve the largest number of customers, would not likely be targeted toward specific requirements for individual customers, and would not be willing to make changes for them. A private cloud could accommodate such needs, but would not meet the criteria for a group working together, and a hybrid cloud spanning multiple cloud providers would not fit the specifics of the question.

QUESTION 3
Data centers have enormous power resources that are distributed and consumed throughout the entire facility.
Which of the following standards pertains to the proper fire safety standards within that scope?

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

Correct Answer: C
Section:
Explanation:

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

QUESTION 4
Which of the following threat types involves an application that does not validate authorization for portions of itself beyond when the user first enters it?

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

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

QUESTION 5
Clustered systems can be used to ensure high availability and load balancing across individual systems through a variety of methodologies.
What process is used within a clustered system to ensure proper load balancing and to maintain the health of the overall system to provide high availability?

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

Correct Answer: D
Section:
Explanation:
Distributed resource scheduling (DRS) is used within all clustered systems as the method for providing high availability, scaling, management, workload distribution, and the balancing of jobs and processes. None of the other choices is the correct term in this case.

QUESTION 6
Although the REST API supports a wide variety of data formats for communications and exchange, which data formats are the most commonly used?

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

Correct Answer: C
Section:
Explanation:
JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API and are typically implemented with caching for increased scalability and performance. Extensible Markup Language (XML) and Security Assertion

Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data. HTML is used for authoring web pages for consumption by web browsers

QUESTION 7

The share phase of the cloud data lifecycle involves allowing data to leave the application, to be shared with external systems, services, or even other vendors/ contractors.
What technology would be useful for protecting data at this point?

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

Correct Answer: B
Section:
Explanation:
Data loss prevention (DLP) solutions allow for control of data outside of the application or original system. They can enforce granular control such as printing, copying, and being read by others, as well as forcing expiration of access. Intrusion detection system (IDS) and intrusion prevention system (IPS) solutions are used for detecting and blocking suspicious and malicious traffic, respectively, whereas a web application firewall (WAF) is used for enforcing security or other controls on web-based applications.

QUESTION 8

When an API is being leveraged, it will encapsulate its data for transmission back to the requesting party or service.
What is the data encapsulation used with the SOAP protocol referred to as?

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

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

QUESTION 9

From a security perspective, what component of a cloud computing infrastructure represents the biggest concern?

A. Hypervisor
B. Management plane
C. Object storage
D. Encryption

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

QUESTION 10

Which of the following is NOT one of the main intended goals of a DLP solution?

A. Showing due diligence
B. Preventing malicious insiders
C. Regulatory compliance
D. Managing and minimizing risk

Correct Answer: B
Section:
Explanation:

Data loss prevention (DLP) extends the capabilities for data protection beyond the standard and traditional security controls that are offered by operating systems, application containers, and network devices. DLP is not specifically implemented to counter malicious insiders, and would not be particularly effective in doing so, because a malicious insider with legitimate access would have other ways to obtain data. DLP is a set of practices and controls to manage and minimize risk, comply with regulatory requirements, and show due diligence with the protection of data.

QUESTION 11

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:
Explanation:

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

QUESTION 12

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:
Explanation:

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

QUESTION 13

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

QUESTION 14
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:
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 15
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:
Explanation:
With multitenancy, eDiscovery becomes more complicated because the data collection involves extra steps to ensure that only those customers or systems that are within scope are turned over to the requesting authority.

QUESTION 16
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:
Explanation:
The functions of the management plane are typically exposed as a series of remote calls and function executions and as a set of APIs. These APIs are typically leveraged through either a client or a web portal, with the latter being the most common.

QUESTION 17
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:
Explanation:
When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, and many times they might be in contention with one other or not clearly applicable. These requirements can include the location of the users and the type of data they enter into systems, the laws governing the organization that owns the application and any regulatory requirements they may have, as well as the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which might be multiple jurisdictions as well.

QUESTION 18
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:
Explanation:
A virtual area network (VLAN) allows the logical separation and isolation of networks and IP spaces to provide enhanced security and controls.

QUESTION 19
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:
Explanation:
The standards put out by Building Industry Consulting Service International (BICSI) primarily cover complex cabling designs and setups for data centers, but also include specifications on power, energy efficiency, and hot/cold aisle setups.

QUESTION 20
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:
Explanation:
The Uptime Institute publishes the most commonly used and widely known standard on data center tiers and topologies. It is based on a series of four tiers, with each progressive increase in number representing more stringent, reliable, and redundant systems for security, connectivity, fault tolerance, redundancy, and cooling.

QUESTION 21
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:
Explanation:
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 22
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:
Explanation:
The Health Insurance Portability and Accountability Act (HIPAA) requires the U.S. Federal Department of Health and Human Services to publish and enforce regulations pertaining to electronic health records and identifiers between patients, providers, and insurance companies. It is focused on the security controls and confidentiality of medical records, rather than the specific technologies used, so long as they meet the requirements of the regulations.

QUESTION 23
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:

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

QUESTION 24
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:
Explanation:
Within IaaS, the number of users on a system is not relevant to the particular hosting model in regard to cloud resources. IaaS is focused on infrastructure needs of a system or application. Therefore, a factor such as the number of users that could affect licensing requirements, for example, would apply to the SaaS model, or in some instances to PaaS.

QUESTION 25
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:
Explanation:
eDiscovery pertains to information and data that is in the possession, control, and custody of an organization.

QUESTION 26
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:
Explanation:
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 27
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:
Explanation:
With static masking, a separate and distinct copy of the data set is created with masking in place. This is typically done through a script or other process that takes a standard data set, processes it to mask the appropriate and predefined fields, and then outputs the data set as a new one with the completed masking done.

QUESTION 28
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:
Explanation:
Structured storage involves organized and categorized data, which most closely resembles and operates like a database system would.

QUESTION 29
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:
Explanation:
The cloud service business manager is responsible for overseeing business plans and customer relationships as well as processing financial transactions.

QUESTION 30
Which protocol does the REST API depend on?

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

Correct Answer: A
Section:

Explanation:
Representational State Transfer (REST) is a software architectural scheme that applies the components, connectors, and data conduits for many web applications used on the Internet. It uses and relies on the HTTP protocol and supports a variety of data formats.

QUESTION 31
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:
Explanation:
Due to the lack of an adequate privacy law or protection at the federal level in the United States, European privacy regulations generally prohibit the exporting or sharing of PII from Europe with the United States. Participation in the Safe Harbor program is voluntary on behalf of an organization, but it does require them to conform to specific requirements and policies that mirror those from the EU. Thus, organizations can fulfill requirements for data sharing and export and possibly serve customers in the EU.

QUESTION 32
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:
Explanation:
When leasing space in a data center, an organization can avoid the enormous startup and building costs associated with a data center, and can instead leverage economies of scale by grouping with other organizations and sharing costs.

QUESTION 33
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:
Explanation:
Trust zones can be implemented to separate systems or tiers along logical lines for great security and access controls. Each zone can then have its own security controls and monitoring based on its particular needs.

QUESTION 34

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:
Explanation:
A cloud customer utilizing proprietary APIs or services from one cloud provider that are unlikely to be available from another cloud provider will most negatively impact portability.

QUESTION 35
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:
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 36
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:
Explanation:
ISO/IEC 27050 strives to establish an internationally accepted standard for eDiscovery processes and best practices. It encompasses all steps of the eDiscovery process: identification, preservation, collection, processing, review, analysis, and the final production of the requested data.

QUESTION 37
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:
Explanation:
The cloud service broker is responsible for obtaining new customers, analyzing the marketplace, and securing contracts and agreements.

QUESTION 38
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:
Explanation:
Forensics is the application of scientific and methodical processes to identify, collect, preserve, analyze, and summarize/report digital information and evidence.

QUESTION 39
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:
Explanation:
The cloud service manager is responsible for the delivery of cloud services, the provisioning of cloud services, and the overall management of cloud services.

QUESTION 40
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:
Explanation:
With international operations, systems ultimately cross many jurisdictional boundaries, and many times, they conflict with each other. The major hurdle to overcome for an organization is the lack of an ultimate international authority to mediate such conflicts, with a likely result of legal efforts in each jurisdiction.

QUESTION 41
GAAPs are created and maintained by which organization?

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

Correct Answer: B
Section:
Explanation:
The AICPA is the organization responsible for generating and maintaining what are the Generally Accepted Accounting Practices in the United States.

QUESTION 42
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:
Explanation:
The cloud service operations manager is responsible for preparing systems for the cloud, administering and monitoring services, providing audit data as requested or required, and managing inventory and assets.

QUESTION 43
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:
Explanation:
iSCSI is a protocol that allows for the transmission and use of SCSI commands and features over a TCP-based network. iSCSI allows systems to use block-level storage that looks and behaves as a SAN would with physical servers, but to leverage the TCP network within a virtualized environment and cloud.

QUESTION 44
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:

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

QUESTION 45
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:
Explanation:
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 46
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:
Explanation:
Any time data is created, modified, or imported, the classification needs to be evaluated and set from the earliest phase to ensure security is always properly maintained for the duration of its lifecycle.

QUESTION 47
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:
Explanation:
The guidelines from ASHRAE establish 64.4-80.6degF (18-27degC) as the optimal temperature for a data center.

QUESTION 48
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:
Explanation:
Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe. The rest are not.

QUESTION 49
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:
Explanation:
Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or where the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with the user's own access and permissions, allowing an attacker to redirect their web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access.

QUESTION 50
How is an object stored within an object storage system?

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

Correct Answer: A
Section:
Explanation:
Object storage uses a flat structure with key values to store and access objects.

QUESTION 51
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:
Explanation:
The payment card industry data security standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry regulatory standard, not a governmental one.

QUESTION 52
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:
Explanation:
The United States lacks a single comprehensive law at the federal level addressing data security and privacy, but there are multiple federal laws that deal with different industries.

QUESTION 53
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:
Explanation:
The GLBA, as it is commonly called based on the lead sponsors and authors of the act, is officially known as "The Financial Modernization Act of 1999." It is specifically focused on PII as it relates to financial institutions. There are three specific components of it, covering various areas and use, on top of a general requirement that all financial institutions must provide all users and customers with a written copy of their privacy policies and practices, including with whom and for what reasons their information may be shared with other entities.

QUESTION 54
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:
Explanation:
Sensitive data exposure occurs when information is not properly secured through encryption and secure transport mechanisms; it can quickly become an easy and broad method for attackers to compromise information. Web applications must enforce strong encryption and security controls on the application side, but secure methods of communications with browsers or other clients used to access the information are also required. Security misconfiguration occurs when applications and systems are not properly configured for security, often a result of misapplied or inadequate baselines. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, thus allowing spoofing for malware or phishing attacks.

QUESTION 55
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:
Explanation:
The best practice is to totally remove any unneeded services and utilities on a system to prevent any chance of compromise or use. If they are just disabled, it is possible for them to be inadvertently started again at any point, or another exploit could be used to start them again. Removing also negates the need to patch and maintain them going forward.

QUESTION 56
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:
Explanation:
Although the initial phase is called "create," it can also refer to modification. In essence, any time data is considered "new," it is in the create phase. This can come from data that is newly created, data that is imported into a system and is new to that system, or data that is already present and modified into a new form or value. Modifying the metadata does not change the actual data.

QUESTION 57
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:
Explanation:
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 58
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:
Explanation:
With many SaaS implementations, data is not isolated to a particular customer but rather is part of the overall application. When it comes to data destruction, a particular challenge is ensuring that all of a customer's data is completely destroyed while not impacting the data of other customers.

QUESTION 59
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:
Explanation:
Some regulations may require specific security controls or certifications be used for hosting certain types of data or functions, and in some circumstances they may be requirements that are unable to be met by any cloud provider.

QUESTION 60
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:
Explanation:
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 61
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:
Explanation:
Limits are put in place to enforce a maximum on the amount of memory or processing a cloud customer can use. This can be done either on a virtual machine or as a comprehensive whole for a customer, and is meant to ensure that enormous cloud resources cannot be allocated or consumed by a single host or customer to the detriment of other hosts and customers.

QUESTION 62
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:
Explanation:
The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated services.

QUESTION 63
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:
Explanation:
Federation pertains to authenticating systems between different organizations.

QUESTION 64
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:

QUESTION 65
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:

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

QUESTION 66
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:
Explanation:
Signed into law and effective starting on September 1, 2015, Russian Law 526-FZ establishes that any collecting, storing, or processing of personal information or data on Russian citizens must be done from systems and databases that are physically located with the Russian Federation.

QUESTION 67
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:
Explanation:
Portability is the ease with which a service or application can be moved between different cloud providers. Maintaining portability gives an organization great flexibility between cloud providers and the ability to shop for better deals or offerings.

QUESTION 68
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:
Explanation:
SOC Type 1 reports are considered "restricted use" reports. They are intended for management and stakeholders of an organization, clients of the service organization, and auditors of the organization. They are not intended for release beyond those audiences.

QUESTION 69
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:
Explanation:
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 70
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:
Explanation:
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 71
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:
Explanation:
An SLA requires performance monitoring of CPU, memory, storage, and networking. The number of users active on a system would not be part of an SLA specifically, other than in regard to the impact on the other four variables.

QUESTION 72
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:
Explanation:
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 73
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:
Explanation:
The recovery point objective (RPO) is defined as the amount of data a company would need to maintain and recover in order to function at a level acceptable to management. This may or may not be a restoration to full operating capacity, depending on what management deems as crucial and essential.

QUESTION 74
What must SOAP rely on for security?

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

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

QUESTION 75
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:
Explanation:
Puppet is a commonly used tool for maintaining system configurations based on policies, and done so from a centralized authority.

QUESTION 76
What type of data does data rights management (DRM) protect?

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

Correct Answer: A
Section:
Explanation:
DRM applies to the protection of consumer media, such as music, publications, video, movies, and soon.

QUESTION 77
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:
Explanation:
Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discovery potential vulnerabilities.

QUESTION 78
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:
Explanation:
When a security professional is considering cloud solutions for BCDR, a top concern is the jurisdiction where the cloud systems are hosted. If the jurisdiction is different from where the production systems are hosted, they may be subjected to different regulations and controls, which would make a seamless BCDR solution far more difficult.

QUESTION 79
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:
Explanation:
In order to obtain and comply with certifications, independent external audits must be performed and satisfied. Although some testing of certification controls can be part of an internal audit, they will not satisfy requirements.

QUESTION 80
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:
Explanation:
Regardless of which cloud-hosting model is used, the cloud customer always has sole responsibility for the data and its security.

QUESTION 81
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:
Explanation:
Dynamic resource scheduling (DRS) is used within all clustering systems as the method for clusters to provide high availability, scaling, management, and workload distribution and balancing of jobs and processes. From a physical infrastructure perspective, DRS is used to balance compute loads between physical hosts in a cloud to maintain the desired thresholds and limits on the physical hosts.

QUESTION 82
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:
Explanation:
The handshake protocol negotiates and establishes the connection as well as handles the key exchange and establishes the session ID. It does not perform the actual encryption of data packets.

QUESTION 83
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:
Explanation:
SOC Type 2 reports are focused on the same policies and procedures, as well as their effectiveness, as SOC Type 1 reports, but are evaluated over a period of at least six consecutive months, rather than a finite point in time.

QUESTION 84
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:
Explanation:
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 85
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:
Explanation:
SOC Type 1 reports are focused specifically on internal controls as they relate to financial reporting.

QUESTION 86
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:
Explanation:

The main goal of confidentiality is to ensure that sensitive information is not made available or leaked to parties that should not have access to it, while at the same time ensuring that those with appropriate need and authorization to access it can do so in a manner commensurate with their needs and confidentiality requirements.

QUESTION 87
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:
Explanation:
Budgetary and cost controls is not one of the domains outlined in the CCM.

QUESTION 88
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:
Explanation:
In any environment, data encryption is incredibly important to prevent unauthorized exposure of data either internally or externally. If a system is compromised by an attack, having the data encrypted on the system will prevent its unauthorized exposure or export, even with the system itself being exposed.

QUESTION 89
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:
Explanation:
Regardless of which cloud-hosting model is used, the cloud provider always has sole responsibility for the physical environment.

QUESTION 90
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:
Explanation:
Firewalls take into account source IP, destination IP, the port the traffic is using, as well as the network protocol (UDP/TCP). Whether or not the traffic is encrypted is not something a firewall is concerned with.

QUESTION 91
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:
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 92
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:
Explanation:
The SOC Type 2 audits include five principles: security, privacy, processing integrity, availability, and confidentiality.

QUESTION 93
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:
Explanation:
With multiple tenants within the same hosting environment, any failure to properly classify data may lead to potential exposure to other customers and applications within the same environment.

QUESTION 94
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:
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 95
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:
Explanation:
Any time a major functional change of an application occurs, a new BCDR test should be done to ensure the overall strategy and process are still applicable and appropriate.

QUESTION 96
What is the biggest challenge to data discovery in a cloud environment?

A. Format
B. Ownership
C. Location
D. Multitenancy

Correct Answer: C
Section:
Explanation:
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 97
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:
Explanation:
Cloud environments depend heavily on API calls for management and automation. Any vulnerability with the APIs can cause significant risk and exposure to all tenants of the cloud environment.

QUESTION 98
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:
Explanation:
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 99
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:
Explanation:
Governance at its core is the idea of assigning jobs, takes, roles, and responsibilities and ensuring they are satisfactory performed.

QUESTION 100
Which regulatory system pertains to the protection of healthcare data?

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

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

QUESTION 101
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:
Explanation:
Cloud environments will regularly change virtual machines as patching and versions are changed. Unlike a physical environment, there is little continuity from one period of time to another. It is very unlikely that the same virtual machines would be in use during a repeat audit.

QUESTION 102
Which security concept would business continuity and disaster recovery fall under?

A. Confidentiality

B. Availability

C. Fault tolerance

D. Integrity

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

QUESTION 103
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:
Explanation:
GitHub is an application for code collaboration, including versioning and branching of code trees. It is not used for applying or maintaining system configurations.

QUESTION 104
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:
Explanation:
Reversibility is the ability for a cloud customer to easily remove their applications or data from a cloud environment, as well as to ensure that all traces of their applications or data have been securely removed per a predefined agreement with the cloud provider.

QUESTION 105
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:
Explanation:
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 106
What concept does the "R" represent with the DREAD model?

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

Correct Answer: A
Section:
Explanation:
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 107
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:
Explanation:
KPIs fall under the "business" aspect of QoS, along with monitoring and measuring of events and business processes. Services, security, and applications are all core components and concepts of the "IT" aspect of QoS.

QUESTION 108
What does dynamic application security testing (DAST) NOT entail?

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

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

QUESTION 109
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:
Explanation:
XML firewalls are most commonly deployed in line between the firewall and application server to validate XML code before it reaches the application.

QUESTION 110
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:
Explanation:
With dynamic masking, production environments are protected with the masking process being implemented between the application and data layers of the application. This allows for a masking translation to take place live in the system and during normal application processing of data.

QUESTION 111
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:
Explanation:
GitHub is an open source tool that developers leverage for code collaboration, branching, and versioning.

QUESTION 112
Which aspect of security is DNSSEC designed to ensure?

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

Correct Answer: A
Section:
Explanation:
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 113
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:
Explanation:
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 114
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:
Explanation:
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 115
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:
Explanation:
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 116
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:
Explanation:
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 117
Which of the following is NOT part of a retention policy?

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

Correct Answer: B
Section:
Explanation:
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 118
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:
Explanation:
Measured service means that costs are only incurred when a cloud customer is actually using cloud services. This is ideal for a business continuity and disaster recovery (BCDR) solution because it negates the need to keep hardware or resources on standby in case of a disaster. Services can be initiated when needed and without costs unless needed.

QUESTION 119
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:
Explanation:
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 120
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:
Explanation:
A host intrusion detection system (HIDS) monitors network traffic as well as critical system files and configurations.

QUESTION 121
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:
Explanation:
An intrusion detection system (IDS) is designed to analyze network packets, compare their contents or characteristics against a set of configurations or signatures, and alert personnel if anything is detected that could constitute a threat or is otherwise designated for alerting.

QUESTION 122

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

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

Correct Answer: A
Section:
Explanation:
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 123
Which attribute of data poses the biggest challenge for data discovery?

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

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

QUESTION 124
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:
Explanation:
Static application security testing (SAST) is conducted with knowledge of the system, including source code, and is done against offline systems.

QUESTION 125
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:
Explanation:
The platform service capability provides programming languages and libraries from the cloud provider, where the customer can deploy their own code and applications into a managed and controlled framework.

QUESTION 126
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:
Explanation:
Dynamic optimization is the process through which the cloud environment is constantly maintained to ensure resources are available when and where needed, and that physical nodes do not become overloaded or near capacity, while others are underutilized.

QUESTION 127
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:
Explanation:
The recovery service level (RSL) is a percentage measure of the total typical production service level that needs to be restored to meet BCDR objectives in the case of a failure.

QUESTION 128
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:
Explanation:
Over time, maintaining the ability to restore and read archives is a primary concern for data archiving. As technologies change and new systems are brought in, it is imperative for an organization to ensure they are still able to restore and access archives for the duration of the required retention period.

QUESTION 129
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:
Explanation:
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 130
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:
Explanation:
A private cloud model, and the specific contractual relationships involved, will give a cloud customer the most level of input and control over how the overall cloud environment is designed and implemented. This would be even more so in cases where the private cloud is owned and operated by the same organization that is hosting services within it.

QUESTION 131
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:
Explanation:
Any application can be a possible target of denial-of-service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for non-authenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks.

QUESTION 132
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:
Explanation:
The cloud service integrator role is responsible for connecting and integrating existing services and applications with cloud-based services.A cloud service administrator is responsible for testing, monitoring, and securing cloud services, as well as providing usage reporting and dealing with service problems. The cloud service user is someone who consumes cloud services. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

QUESTION 133
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:
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 134
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:
Explanation:
The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and accounting errors.The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy. The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Safe Harbor program was designed by the US government as a way for American companies to comply with European Union privacy laws.

QUESTION 135
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:
Explanation:
A cross-site request forgery (CSRF) attack forces a client that a user has used to authenticate to an application to send forged requests under the user's own credentials to execute commands and requests that the application thinks are coming from a trusted client and user. Although this type of attack cannot be used to steal data directly because the attacker has no way of seeing the results of the commands, it does open other ways to compromise an application. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries.

QUESTION 136
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:
Explanation:
Platform as a Service would allow software developers to quickly and easily deploy their applications among different hosting providers for testing and validation in order to determine the best option. Although IaaS would also be appropriate for hosting applications, it would require too much configuration of application servers and libraries in order to test code. Conversely, PaaS would provide a ready-to-use environment from the onset. DaaS would not be appropriate in any way for software developers to use to deploy applications. IaaS would not be appropriate in this scenario because it would require the developers to also deploy and maintain the operating system images or to contract with another firm to do so. SaaS, being a fully functional software platform, would not be appropriate for deploying applications into.

QUESTION 137
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:
Explanation:
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 138
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:
Explanation:
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 139
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:
Explanation:
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 140
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:
Explanation:
Regardless of the particular cloud service used, physical security of hardware and facilities is always the sole responsibility of the cloud provider. The cloud provider may release information about their physical security policies and procedures to ensure any particular requirements of potential customers will meet their regulatory obligations. Personal security of developers and regulatory compliance are always the responsibility of the cloud customer. Responsibility for operating systems, and the auditing of them, will differ based on the cloud service category used.

QUESTION 141
Humidity levels for a data center are a prime concern for maintaining electrical and computing resources properly as well as ensuring that conditions are optimal for top performance.
Which of the following is the optimal humidity level, as established by ASHRAE?

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

Correct Answer: C
Section:
Explanation:
The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) recommends 40 to 60 percent relatively humidity for data centers.
None of these options is the recommendation from ASHRAE.

QUESTION 142
Within a SaaS environment, what is the responsibility on the part of the cloud customer in regard to procuring the software used?

A. Maintenance
B. Licensing
C. Development
D. Purchasing

Correct Answer: B
Section:
Explanation:
Within a SaaS implementation, the cloud customer licenses the use of the software from the cloud provider because SaaS delivers a fully functional application to the customer. With SaaS, the cloud provider is responsible for the entire software application and any necessary infrastructure to develop, run, and maintain it. The purchasing, development, and maintenance are fully the responsibility of the cloud provider.

QUESTION 143
Implementing baselines on systems would take an enormous amount of time and resources if the staff had to apply them to each server, and over time, it would be almost impossible to keep all the systems in sync on an ongoing basis.
Which of the following is NOT a package that can be used for implementing and maintaining baselines across an enterprise?

A. Puppet
B. SCCM
C. Chef
D. GitHub

Correct Answer: D
Section:
Explanation:
GitHub is a software development platform that serves as a code repository and versioning system. It is solely used for software development and would not be appropriate for applying baselines to systems. Puppet is an open-source configuration management tool that runs on many platforms and can be used to apply and maintain baselines. The Software Center Configuration Manager (SCCM) was developed by Microsoft for managing systems across large groups of servers.
Chef is also a system for maintaining large groups of systems throughout an enterprise.

QUESTION 144
From the perspective of compliance, what is the most important consideration when it comes to data center location?

A. Natural disasters
B. Utility access

C. Jurisdiction
D. Personnel access

Correct Answer: C
Section:
Explanation:
Jurisdiction will dictate much of the compliance and audit requirements for a data center. Although all the aspects listed are very important to security, from a strict compliance perspective, jurisdiction is the most important. Personnel access, natural disasters, and utility access are all important operational considerations for selecting a data center location, but they are not related to compliance issues like jurisdiction is.

QUESTION 145
Different certifications and standards take different approaches to data center design and operations. Although many traditional approaches use a tiered methodology, which of the following utilizes a macro-level approach to data center design?

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

Correct Answer: A
Section:
Explanation:
The Infinity Paradigm of the International Data Center Authority (IDCA) takes a macro-level approach to data center design. The IDCA does not use a specific, focused approach on specific components to achieve tier status. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. The
Uptime Institute publishes the most widely known and used standard for data center topologies and tiers.

QUESTION 146
The European Union is often considered the world leader in regard to the privacy of personal data and has declared privacy to be a "human right." In what year did the EU first assert this principle?

A. 1995
B. 2000
C. 2010
D. 1999

Correct Answer: A
Section:
Explanation:
The EU passed Directive 95/46 EC in 1995, which established data privacy as a human right. The other years listed are incorrect.

QUESTION 147
A DLP solution/implementation has three main components.
Which of the following is NOT one of the three main components?

A. Monitoring
B. Enforcement
C. Auditing
D. Discovery and classification

Correct Answer: C
Section:
Explanation:
Auditing, which can be supported to varying degrees by DLP solutions, is not a core component of them. Data loss prevention (DLP) solutions have core components of discovery and classification, enforcement, and monitoring. Discovery and classification are concerned with determining which data should be applied to the DLP policies, and then determining its classification level. Monitoring is concerned with the actual watching of data and how it's used through its various stages. Enforcement is the actual application of policies determined from the discovery stage and then triggered during the monitoring stage.

QUESTION 148
What type of storage structure does object storage employ to maintain files?

A. Directory
B. Hierarchical
C. tree
D. Flat

Correct Answer: D
Section:
Explanation:
Object storage uses a flat file system to hold storage objects; it assigns files a key value that is then used to access them, rather than relying on directories or descriptive filenames. Typical storage layouts such as tree, directory, and hierarchical structures are used within volume storage, whereas object storage maintains a flat structure with key values.

QUESTION 149
Data center and operations design traditionally takes a tiered, topological approach.
Which of the following standards is focused on that approach and is prevalently used throughout the industry?

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

Correct Answer: D
Section:
Explanation:
The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers. The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The International Data Center Authority (IDCA) offers the Infinity Paradigm, which takes a macro-level approach to data center design.

QUESTION 150
Jurisdictions have a broad range of privacy requirements pertaining to the handling of personal data and information.
Which jurisdiction requires all storage and processing of data that pertains to its citizens to be done on hardware that is physically located within its borders?

A. Japan
B. United States
C. European Union
D. Russia

Correct Answer: D
Section:

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

QUESTION 151
The management plane is used to administer a cloud environment and perform administrative tasks across a variety of systems, but most specifically it's used with the hypervisors.
What does the management plane typically leverage for this orchestration?

A. APIs
B. Scripts
C. TLS
D. XML

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

QUESTION 152
When dealing with PII, which category pertains to those requirements that can carry legal sanctions or penalties for failure to adequately safeguard the data and address compliance requirements?

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

Correct Answer: C
Section:
Explanation:
Regulated PII pertains to data that is outlined in law and regulations. Violations of the requirements for the protection of regulated PII can carry legal sanctions or penalties. Contractual PII involves required data protection that is determined by the actual service contract between the cloud provider and cloud customer, rather than outlined by law. Violations of the provisions of contractual PII carry potential financial or contractual implications, but not legal sanctions. Legal and jurisdictional are similar terms to regulated, but neither is the official term used.

QUESTION 153
Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.
Which of the following is NOT a regulatory system from the United States federal government?

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

Correct Answer: D
Section:
Explanation:
The Payment Card Industry Data Security Standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry-regulatory standard, not a governmental one. The Sarbanes-Oxley Act (SOX) was

passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders. The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

QUESTION 154
The president of your company has tasked you with implementing cloud services as the most efficient way of obtaining a robust disaster recovery configuration for your production services.
Which of the cloud deployment models would you MOST likely be exploring?

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

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

QUESTION 155
If you are running an application that has strict legal requirements that the data cannot reside on systems that contain other applications or systems, which aspect of cloud computing would be prohibitive in this case?

A. Multitenancy
B. Broad network access
C. Portability
D. Elasticity

Correct Answer: A
Section:
Explanation:
Multitenancy is the aspect of cloud computing that involves having multiple customers and applications running within the same system and sharing the same resources. Although considerable mechanisms are in place to ensure isolation and separation, the data and applications are ultimately using shared resources.
Broad network access refers to the ability to access cloud services from any location or client. Portability refers to the ability to easily move cloud services between different cloud providers, whereas elasticity refers to the capabilities of a cloud environment to add or remove services, as needed, to meet current demand.

QUESTION 156
The REST API is a widely used standard for communications of web-based services between clients and the servers hosting them.
Which protocol does the REST API depend on?

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

Correct Answer: A
Section:
Explanation:

Representational State Transfer (REST) is a software architectural scheme that applies the components, connectors, and data conduits for many web applications used on the Internet. It uses and relies on the HTTP protocol and supports a variety of data formats. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data. Secure Shell client (SSH) is a secure method for allowing remote login to systems over a network.

QUESTION 157
Which of the following actions will NOT make data part of the create phase of the cloud data lifecycle?

A. Modify data
B. Modify metadata
C. New data
D. Import data

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

QUESTION 158
Most APIs will support a variety of different data formats or structures.
However, the SOAP API will only support which one of the following data formats?

A. XML
B. XSLT
C. JSON
D. SAML

Correct Answer: A
Section:
Explanation:
The Simple Object Access Protocol (SOAP) protocol only supports the Extensible Markup Language (XML) data format. Although the other options are all data formats or data structures, they are not supported by SOAP.

QUESTION 159
Which cloud storage type is typically used to house virtual machine images that are used throughout the environment?

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

Correct Answer: D
Section:
Explanation:
Object storage is typically used to house virtual machine images because it is independent from other systems and is focused solely on storage. It is also the most appropriate for handling large individual files. Volume storage, because it is allocated to a specific host, would not be appropriate for the storing of virtual images. Structured and unstructured are storage types specific to PaaS and would not be used for storing items used throughout a cloud environment.

QUESTION 160

Many activities within a cloud environment are performed via programmatic means, where complex and distributed operations are handled without the need to perform each step individually.
Which of the following concepts does this describe?

A. Orchestration
B. Provisioning
C. Automation
D. Allocation

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

QUESTION 161
Being in a cloud environment, cloud customers lose a lot of insight and knowledge as to how their data is stored and their systems are deployed. Which concept from the ISO/IEC cloud standards relates to the necessity of the cloud provider to inform the cloud customer on these issues?

A. Disclosure
B. Transparency
C. Openness
D. Documentation

Correct Answer: B
Section:
Explanation:
Transparency is the official process by which a cloud provider discloses insight and information into its configurations or operations to the appropriate audiences. Disclosure, openness, and documentation are all terms that sound similar to the correct answer, but none of them is the correct term in this case.

QUESTION 162
Your IT steering committee has, at a high level, approved your project to begin using cloud services. However, the committee is concerned with getting locked into a single cloud provider and has flagged the ability to easily move between cloud providers as a top priority. It also wants to save costs by reusing components.
Which cross-cutting aspect of cloud computing would be your primary focus as your project plan continues to develop and you begin to evaluate cloud providers?

A. Interoperability
B. Resiliency
C. Scalability
D. Portability

Correct Answer: A
Section:
Explanation:
Interoperability is ability to easily move between cloud providers, by either moving or reusing components and services. This can pertain to any cloud deployment model, and it gives organizations the ability to constantly evaluate costs and services as well as move their business to another cloud provider as needed or desired. Portability relates to the wholesale moving of services from one cloud provider to another, not necessarily the reuse of components or services for other purposes. Although resiliency is not an official concept within cloud computing, it certainly would be found throughout other topics such as elasticity, auto-scaling, and resource pooling. Scalability pertains to changing resource allocations to a service to meet current demand, either upward or downward in scope.

QUESTION 163

Which of the following provides assurance, to a predetermined acceptable level of certainty, that an entity is indeed who they claim to be?

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

Correct Answer: A
Section:
Explanation:
Authentication goes a step further than identification by providing a means for proving an entity's identification. Authentication is most commonly done through mechanisms such as passwords. Identification involves ascertaining who the entity is, but without a means of proving it, such as a name or user ID. Authorization occurs after authentication and sets access permissions and other privileges within a system or application for the user. Proofing is not a term that is relevant to the question.

QUESTION 164
Whereas a contract articulates overall priorities and requirements for a business relationship, which artifact enumerates specific compliance requirements, metrics, and response times?

A. Service level agreement
B. Service level contract
C. Service compliance contract
D. Service level amendment

Correct Answer: A
Section:
Explanation:

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

QUESTION 165
When an organization is considering the use of cloud services for BCDR planning and solutions, which of the following cloud concepts would be the most important?

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

Correct Answer: D
Section:
Explanation:
Portability is the ability for a service or system to easily move among different cloud providers. This is essential for using a cloud solution for BCDR because vendor lock-in would inhibit easily moving and setting up services in the event of a disaster, or it would necessitate a large number of configuration or component changes to implement. Interoperability, or the ability to reuse components for other services or systems, would not be an important factor for BCDR.
Reversibility, or the ability to remove all data quickly and completely from a cloud environment, would be important at the end of a disaster, but would not be important during setup and deployment. Elasticity, or the ability to resize resources to meet current demand, would be very beneficial to a BCDR situation, but not as vital as portability.

QUESTION 166
What masking strategy involves the replacing of sensitive data at the time it is accessed and used as it flows between the data and application layers of a service?

A. Active
B. Static
C. Dynamic
D. Transactional

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

QUESTION 167
Which of the following would be considered an example of insufficient due diligence leading to security or operational problems when moving to a cloud?

A. Monitoring
B. Use of a remote key management system
C. Programming languages used
D. Reliance on physical network controls

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

QUESTION 168
Which aspect of cloud computing serves as the biggest challenge to using DLP to protect data at rest?

A. Portability
B. Resource pooling
C. Interoperability
D. Reversibility

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

QUESTION 169
What category of PII data can carry potential fines or even criminal charges for its improper use or disclosure?

A. Protected
B. Legal
C. Regulated

D. Contractual

Correct Answer: C
Section:
Explanation:
Regulated PII data carries legal and jurisdictional requirements, along with official penalties for its misuse or disclosure, which can be either civil or criminal in nature. Legal and protected are similar terms, but neither is the correct answer in this case. Contractual requirements can carry financial or contractual impacts for the improper use or disclosure of PII data, but not legal or criminal penalties that are officially enforced.

QUESTION 170
A variety of security systems can be integrated within a network--some that just monitor for threats and issue alerts, and others that take action based on signatures, behavior, and other types of rules to actively stop potential threats.
Which of the following types of technologies is best described here?

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

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

QUESTION 171
Upon completing a risk analysis, a company has four different approaches to addressing risk. Which approach it takes will be based on costs, available options, and adherence to any regulatory requirements from independent audits.
Which of the following groupings correctly represents the four possible approaches?

A. Accept, avoid, transfer, mitigate
B. Accept, deny, transfer, mitigate
C. Accept, deny, mitigate, revise
D. Accept, dismiss, transfer, mitigate

Correct Answer: A
Section:
Explanation:
The four possible approaches to risk are as follows: accept (do not patch and continue with the risk), avoid (implement solutions to prevent the risk from occurring), transfer (take out insurance), and mitigate (change configurations or patch to resolve the risk). Each of these answers contains at least one incorrect approach name.

QUESTION 172
Which of the following is NOT a component of access control?

A. Accounting
B. Federation
C. Authorization
D. Authentication

Correct Answer: B
Section:
Explanation:
Federation is not a component of access control. Instead, it is used to allow users possessing credentials from other authorities and systems to access services outside of their domain. This allows for access and trust without the need to create additional, local credentials. Access control encompasses not only the key concepts of authorization and authentication, but also accounting. Accounting consists of collecting and maintaining logs for both authentication and authorization for operational and regulatory requirements.

QUESTION 173
What concept does the A represent within the DREAD model?

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

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

QUESTION 174
With an application hosted in a cloud environment, who could be the recipient of an eDiscovery order?

A. Users
B. Both the cloud provider and cloud customer
C. The cloud customer
D. The cloud provider

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

QUESTION 175
Which ITIL component focuses on ensuring that system resources, processes, and personnel are properly allocated to meet SLA requirements?

A. Continuity management
B. Availability management
C. Configuration management
D. Problem management

Correct Answer: B
Section:
Explanation:
Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Configuration management tracks and maintains detailed information about all IT components within an organization.

Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

QUESTION 176

Which ITIL component is an ongoing, iterative process of tracking all deployed and configured resources that an organization uses and depends on, whether they are hosted in a traditional data center or a cloud?

A. Problem management
B. Continuity management
C. Availability management
D. Configuration management

Correct Answer: D
Section:
Explanation:

Configuration management tracks and maintains detailed information about all IT components within an organization. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster.

Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

QUESTION 177

When beginning an audit, both the system owner and the auditors must agree on various aspects of the final audit report.
Which of the following would NOT be something that is predefined as part of the audit agreement?

A. Size
B. Format
C. Structure
D. Audience

Correct Answer: A
Section:
Explanation:

The ultimate size of the audit report is not something that would ever be included in the audit scope or definition. Decisions about the content of the report should be the only factor that drives the ultimate size of the report.
The structure, audience, and format of the audit report are all crucial elements that must be defined and agreed upon as part of the audit scope.

QUESTION 178

What concept does the D represent within the STRIDE threat model?

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

Correct Answer: A
Section:
Explanation:

Any application can be a possible target of denial of service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for unauthenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks. None of the other options provided is the correct term.

QUESTION 179

Which of the following is the concept of segregating information or processes, within the same system or application, for security reasons?

A. Cell blocking
B. Sandboxing
C. Pooling
D. Fencing

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

QUESTION 180
Which cloud service category most commonly uses client-side key management systems?

A. Software as a Service
B. Infrastructure as a Service
C. Platform as a Service
D. Desktop as a Service

Correct Answer: A
Section:
Explanation:
SaaS most commonly uses client-side key management. With this type of implementation, the software for doing key management is supplied by the cloud provider, but is hosted and run by the cloud customer. This allows for full integration with the SaaS implementation, but also provides full control to the cloud customer. Although the cloud provider may offer software for performing key management to the cloud customers, with the Infrastructure, Platform, and Desktop as a Service categories, the customers would largely be responsible for their own options and implementations and would not be bound by the offerings from the cloud provider.

QUESTION 181
Apart from using encryption at the file system level, what technology is the most widely used to protect data stored in an object storage system?

A. TLS
B. HTTPS
C. VPN
D. IRM

Correct Answer: D
Section:
Explanation:
Information rights management (IRM) technologies allow security controls and policies to be enforced on a data object regardless of where it resides. They also allow for extended controls such as expirations and copying restrictions, which are not available through traditional control mechanisms. Hypertext Transfer Protocol Secure (HTTPS), virtual private network (VPN), and Transport Layer Security (TLS) are all technologies and protocols that are widely used with cloud implementations for secure access to systems and services and likely will be used in conjunction with other object data protection strategies.

QUESTION 182
Which of the following types of data would fall under data rights management (DRM) rather than information rights management (IRM)?

A. Personnel data

B. Security profiles
C. Publications
D. Financial records

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

QUESTION 183
Different security testing methodologies offer different strategies and approaches to testing systems, requiring security personnel to determine the best type to use for their specific circumstances.
What does dynamic application security testing (DAST) NOT entail that SAST does?

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

Correct Answer: B
Section:
Explanation:
Dynamic application security testing (DAST) is considered "black-box" testing and begins with no inside knowledge of the application or its configurations.
Everything about it must be discovered during its testing. As with most types of testing, dynamic application security testing (DAST) involves probing, scanning, and a discovery process for system information.

QUESTION 184
You need to gain approval to begin moving your company's data and systems into a cloud environment. However, your CEO has mandated the ability to easily remove your IT assets from the cloud provider as a precondition.
Which of the following cloud concepts would this pertain to?

A. Removability
B. Extraction
C. Portability
D. Reversibility

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

QUESTION 185
What does static application security testing (SAST) offer as a tool to the testers that makes it unique compared to other common security testing methodologies?

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

D. Injection attempts

Correct Answer: B
Section:
Explanation:
Static application security testing (SAST) is conducted against offline systems with previous knowledge of them, including their source code. Live testing is not part of static testing but rather is associated with dynamic testing. Production system scanning is not appropriate because static testing is done against offline systems. Injection attempts are done with many different types of testing and are not unique to one particular type. It is therefore not the best answer to the question.

QUESTION 186
A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence.
Which core concept of cloud computing is most related to vendor lock-in?

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

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

QUESTION 187
Which of the following areas of responsibility always falls completely under the purview of the cloud provider, regardless of which cloud service category is used?

A. Infrastructure
B. Data
C. Physical
D. Governance

Correct Answer: C
Section:
Explanation:
Regardless of the cloud service category used, the physical environment is always the sole responsibility of the cloud provider. In many instances, the cloud provider will supply audit reports or some general information about their physical security practices, especially to those customers or potential customers that may have regulatory requirements, but otherwise the cloud customer will have very little insight into the physical environment. With IaaS, the infrastructure is a shared responsibility between the cloud provider and cloud customer. With all cloud service categories, the data and governance are always the sole responsibility of the cloud customer.

QUESTION 188
What type of masking would you employ to produce a separate data set for testing purposes based on production data without any sensitive information?

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

Correct Answer: D
Section:
Explanation:
Static masking involves taking a data set and replacing sensitive fields and values with non-sensitive or garbage data. This is done to enable testing of an application against data that resembles production data, both in size and format, but without containing anything sensitive. Dynamic masking involves the live and transactional masking of data while an application is using it. Tokenized would refer to tokenization, which is the replacing of sensitive data with a key value that can later be matched back to the original value, and although it could be used as part of the production of test data, it does not refer to the overall process.
Replicated is provided as an erroneous answer, as replicated data would be identical in value and would not accomplish the production of a test set.

QUESTION 189
Which aspect of data poses the biggest challenge to using automated tools for data discovery and programmatic data classification?

A. Quantity
B. Language
C. Quality
D. Number of courses

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

QUESTION 190
When an organization is considering a cloud environment for hosting BCDR solutions, which of the following would be the greatest concern?

A. Self-service
B. Resource pooling
C. Availability
D. Location

Correct Answer: D
Section:
Explanation:
If an organization wants to use a cloud service for BCDR, the location of the cloud hosting becomes a very important security consideration due to regulations and jurisdiction, which could be dramatically different from the organization's normal hosting locations. Availability is a hallmark of any cloud service provider, and likely will not be a prime consideration when an organization is considering using a cloud for BCDR; the same goes for self-service options. Resource pooling is common among all cloud systems and would not be a concern when an organization is dealing with the provisioning of resources during a disaster.

QUESTION 191
Just like the risk management process, the BCDR planning process has a defined sequence of steps and processes to follow to ensure the production of a comprehensive and successful plan.
Which of the following is the correct sequence of steps for a BCDR plan?

A. Define scope, gather requirements, assess risk, implement
B. Define scope, gather requirements, implement, assess risk
C. Gather requirements, define scope, implement, assess risk
D. Gather requirements, define scope, assess risk, implement

Correct Answer: A
Section:
Explanation:
The correct sequence for a BCDR plan is to define the scope, gather requirements based on the scope, assess overall risk, and implement the plan. The other sequences provided are not in the correct order.

QUESTION 192
What type of solution is at the core of virtually all directory services?

A. WS
B. LDAP
C. ADFS
D. PKI

Correct Answer: B
Section:
Explanation:
The Lightweight Directory Access Protocol (LDAP) forms the basis of virtually all directory services, regardless of the specific vendor or software package.WS is a protocol for information exchange between two systems and does not actually store the data. ADFS is a Windows component for enabling single sign-on for the operating system and applications, but it relies on data from an LDAP server. PKI is used for managing and issuing security certificates.

QUESTION 193
The different cloud service models have varying levels of responsibilities for functions and operations depending with the model's level of service.
In which of the following models would the responsibility for patching lie predominantly with the cloud customer?

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

Correct Answer: D
Section:
Explanation:
With Infrastructure as a Service (IaaS), the cloud customer is responsible for deploying and maintaining its own systems and virtual machines. Therefore, the customer is solely responsible for patching and any other security updates it finds necessary. With Software as a Service (SaaS), Platform as a Service (PaaS), and Desktop as a Service (DaaS), the cloud provider maintains the infrastructure components and is responsible for maintaining and patching them.

QUESTION 194
Which component of ITIL involves the creation of an RFC ticket and obtaining official approvals for it?

A. Problem management
B. Release management
C. Deployment management
D. Change management

Correct Answer: D
Section:
Explanation:
The change management process involves the creation of the official Request for Change (RFC) ticket, which is used to document the change, obtain the required approvals from management and stakeholders, and track the

change to completion. Release management is a subcomponent of change management, where the actual code or configuration change is put into place. Deployment management is similar to release management, but it's where changes are actually implemented on systems. Problem management is focused on the identification and mitigation of known problems and deficiencies before they are able to occur.

QUESTION 195
Which of the following are attributes of cloud computing?

A. Minimal management effort and shared resources
B. High cost and unique resources
C. Rapid provisioning and slow release of resources
D. Limited access and service provider interaction

Correct Answer: A
Section:
Explanation:
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

QUESTION 196
In a cloud environment, encryption should be used for all the following, except:

A. Secure sessions/VPN
B. Long-term storage of data
C. Near-term storage of virtualized images
D. Profile formatting

Correct Answer: D
Section:
Explanation:
All of these activities should incorporate encryption, except for profile formatting, which is a made-up term.

QUESTION 197
Which of the following is considered a technological control?

A. Firewall software
B. Firing personnel
C. Fireproof safe
D. Fire extinguisher

Correct Answer: A
Section:
Explanation:
A firewall is a technological control. The safe and extinguisher are physical controls and firing someone is an administrative control.

QUESTION 198
When using an IaaS solution, what is the capability provided to the customer?

A. To provision processing, storage, networks, and other fundamental computing resources when the consumer is able to deploy and run arbitrary software, which can include OSs and applications.

B. To provision processing, storage, networks, and other fundamental computing resources when the auditor is able to deploy and run arbitrary software, which can include OSs and applications.

C. To provision processing, storage, networks, and other fundamental computing resources when the provider is able to deploy and run arbitrary software, which can include OSs and applications.

D. To provision processing, storage, networks, and other fundamental computing resources when the consumer is not able to deploy and run arbitrary software, which can include OSs and applications.

Correct Answer: A
Section:
Explanation:
According to "The NIST Definition of Cloud Computing," in IaaS, "the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

QUESTION 199
When using an IaaS solution, what is a key benefit provided to the customer?

A. Metered and priced on the basis of units consumed

B. Increased energy and cooling system efficiencies

C. Transferred cost of ownership

D. The ability to scale up infrastructure services based on projected usage

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

QUESTION 200
Which of the following is considered an administrative control?

A. Keystroke logging

B. Access control process

C. Door locks

D. Biometric authentication

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

QUESTION 201
What is a key capability or characteristic of PaaS?

A. Support for a homogenous environment

B. Support for a single programming language

C. Ability to reduce lock-in

D. Ability to manually scale

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

QUESTION 202
In which cloud service model is the customer required to maintain the OS?

A. Iaas
B. CaaS
C. PaaS
D. SaaS

Correct Answer: A
Section:
Explanation:
In IaaS, the service is bare metal, and the customer has to install the OS and the software; the customer then is responsible for maintaining that OS. In the other models, the provider installs and maintains the OS.

QUESTION 203
When using a PaaS solution, what is the capability provided to the customer?

A. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the provider supports. The provider does not manage or control the underlyingcloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
B. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the provider supports. The consumer does not manage or control the underlyingcloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
C. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the consumer supports. The consumer does not manage or control the underlyingcloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
D. To deploy onto the cloud infrastructure provider-created or acquired applications created using programming languages, libraries, services, and tools that the provider supports. The consumer does not manage or control the underlyingcloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Correct Answer: B
Section:

Explanation:
According to "The NIST Definition of Cloud Computing," in PaaS, "the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

QUESTION 204
What are SOC 1/SOC 2/SOC 3?

A. Audit reports
B. Risk management frameworks
C. Access controls
D. Software developments

Correct Answer: A
Section:
Explanation:
An SOC 1 is a report on controls at a service organization that may be relevant to a user entity's internal control over financial reporting. An SOC 2 report is based on the existing SysTrust and WebTrust principles. The purpose of an SOC 2 report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, or privacy. An SOC 3 report is also based on the existing SysTrust and WebTrust principles, like a SOC 2 report. The difference is that the SOC 3 report does not detail the testing performed.

QUESTION 205
Gathering business requirements can aid the organization in determining all of this information about organizational assets, except:

A. Full inventory
B. Criticality
C. Value
D. Usefulness

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

QUESTION 206
In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?

A. Physical
B. All of the above
C. technological
D. Administrative

Correct Answer: B
Section:
Explanation:
Layered defense calls for a diverse approach to security.

QUESTION 207

The BIA can be used to provide information about all the following, except:

A. BC/DR planning
B. Risk analysis
C. Secure acquisition
D. Selection of security controls

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

QUESTION 208
Which of the following are cloud computing roles?

A. Cloud service broker and user
B. Cloud customer and financial auditor
C. CSP and backup service provider
D. Cloud service auditor and object

Correct Answer: C
Section:
Explanation:

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

QUESTION 209
Which of the following are considered to be the building blocks of cloud computing?

A. CPU, RAM, storage, and networking
B. Data, CPU, RAM, and access control
C. Data, access control, virtualization, and services
D. Storage, networking, printing, and virtualization

Correct Answer: A
Section:

QUESTION 210
Which of the following is considered a physical control?

A. Fences
B. Ceilings
C. Carpets
D. Doors

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

QUESTION 211
What is an experimental technology that is intended to create the possibility of processing encrypted data without having to decrypt it first?

A. Quantum-state
B. Polyinstantiation
C. Homomorphic
D. Gastronomic

Correct Answer: C
Section:
Explanation:
Homomorphic encryption hopes to achieve that goal; the other options are terms that have almost nothing to do with encryption.

QUESTION 212
Which of the following are distinguishing characteristics of a managed service provider?

A. Be able to remotely monitor and manage objects for the customer and proactively maintain these objects under management.
B. Have some form of a help desk but no NOC.
C. Be able to remotely monitor and manage objects for the customer and reactively maintain these objects under management.
D. Have some form of a NOC but no help desk.

Correct Answer: A
Section:
Explanation:
According to the MSP Alliance, typically MSPs have the following distinguishing characteristics:
- Have some form of NOC service
- Have some form of help desk service
- Can remotely monitor and manage all or a majority of the objects for the customer
- Can proactively maintain the objects under management for the customer
- Can deliver these solutions with some form of predictable billing model, where the customer knows with great accuracy what her regular IT management expense will be

QUESTION 213
To protect data on user devices in a BYOD environment, the organization should consider requiring all the following, except:

A. Multifactor authentication
B. DLP agents

C. Two-person integrity
D. Local encryption

Correct Answer: C
Section:
Explanation:
Although all the other options are ways to harden a mobile device, two-person integrity is a concept that has nothing to do with the topic, and, if implemented, would require everyone in your organization to walk around in pairs while using their mobile devices.

QUESTION 214
Tokenization requires two distinct __________________ .

A. Authentication factors
B. Personnel
C. Databases
D. Encryption

Correct Answer: C
Section:
Explanation:
In order to implement tokenization, there will need to be two databases: the database containing the raw, original data, and the token database containing tokens that map to original data. Having two-factor authentication is nice, but certainly not required. Encryption keys are not necessary for tokenization. Two-person integrity does not have anything to do with tokenization.

QUESTION 215
DLP can be combined with what other security technology to enhance data controls?

A. DRM
B. Hypervisor
C. SIEM
D. Kerberos

Correct Answer: A
Section:
Explanation:
DLP can be combined with DRM to protect intellectual property; both are designed to deal with data that falls into special categories. SIEMs are used for monitoring event logs, not live data movement. Kerberos is an authentication mechanism. Hypervisors are used for virtualization.

QUESTION 216
What is the intellectual property protection for a confidential recipe for muffins?

A. Patent
B. Trademark
C. Trade secret
D. Copyright

Correct Answer: C
Section:
Explanation:

Confidential recipes unique to the organization are trade secrets. The other answers listed are answers to other questions.

QUESTION 217
Every security program and process should have which of the following?

A. Severe penalties
B. Multifactor authentication
C. Foundational policy
D. Homomorphic encryption

Correct Answer: C
Section:
Explanation:
Policy drives all programs and functions in the organization; the organization should not conduct any operations that don't have a policy governing them.
Penalties may or may not be an element of policy, and severity depends on the topic. Multifactor authentication and homomorphic encryption are red herrings here.

QUESTION 218
DLP solutions can aid in deterring loss due to which of the following?

A. Inadvertent disclosure
B. Natural disaster
C. Randomization
D. Device failure

Correct Answer: A
Section:
Explanation:
DLP solutions may protect against inadvertent disclosure. Randomization is a technique for obscuring data, not a risk to data. DLP tools will not protect against risks from natural disasters, or against impacts due to device failure.

QUESTION 219
All policies within the organization should include a section that includes all of the following, except:

A. Policy adjudication
B. Policy maintenance
C. Policy review
D. Policy enforcement

Correct Answer: A
Section:
Explanation:
All the elements except adjudication need to be addressed in each policy. Adjudication is not an element of policy.

QUESTION 220
Proper implementation of DLP solutions for successful function requires which of the following?

A. Physical access limitations

B. USB connectivity
C. Accurate data categorization
D. Physical presence

Correct Answer: C
Section:
Explanation:
DLP tools need to be aware of which information to monitor and which requires categorization (usually done upon data creation, by the data owners). DLPs can be implemented with or without physical access or presence. USB connectivity has nothing to do with DLP solutions.

QUESTION 221
What is the experimental technology that might lead to the possibility of processing encrypted data without having to decrypt it first?

A. AES
B. Link encryption
C. One-time pads
D. Homomorphic encryption

Correct Answer: D
Section:
Explanation:
AES is an encryption standard. Link encryption is a method for protecting communications traffic. One-time pads are an encryption method.