CCSP.exam.258q

Number: CCSP
Passing Score: 800
Time Limit: 120 min
File Version: 1

ISC CCSP

Certified Cloud Security Professional (CCSP)

Exam A

QUESTION 1
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: (none)
Explanation

Explanation/Reference:
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 2
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: (none)
Explanation

Explanation/Reference:
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 3
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: (none)
Explanation

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

QUESTION 4
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: (none)
Explanation

Explanation/Reference:
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 5
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:**
(none) Explanation

Explanation/Reference:
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 6
The REST API is a widely used standard for communications of web-based services between clients and the servers hosting them.

Which protocol does the REST API depend on?
A. HTTP
B. SSH
C. SAML
D. XML

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 7
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:**
(none) Explanation

Explanation/Reference:
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 8
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: (none)
Explanation

Explanation/Reference:
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 9
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: (none)
Explanation

Explanation/Reference:
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 10
With an API, various features and optimizations are highly desirable to scalability, reliability, and security.

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

A. Acceleration
B. Caching
C. Redundancy
D. Encryption

Correct Answer: B **Section:**
(none) Explanation

Explanation/Reference:
Explanation:
The Simple Object Access Protocol (SOAP) does not support caching, whereas the Representational State Transfer (REST) API does. The other options are all capabilities that are either not supported by SOAP or not supported by any API and must be provided by external features.

QUESTION 11
Although much of the attention given to data security is focused on keeping data private and only accessible by authorized individuals, of equal importance is the trustworthiness of the data.

Which concept encapsulates this?

A. Validity
B. Integrity
C. Accessibility
D. Confidentiality

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Integrity refers to the trustworthiness of data and whether its format and values are true and have not been corrupted or otherwise altered through unauthorized means. Confidentiality refers to keeping data from being access or viewed by unauthorized parties. Accessibility means that data is available and ready when needed by a user or service. Validity can mean a variety of things that are somewhat similar to integrity, but it's not the most appropriate answer in this case.

QUESTION 12
Three central concepts define what type of data and information an organization is responsible for pertaining to eDiscovery.

Which of the following are the three components that comprise required disclosure?

A. Possession, ownership, control
B. Ownership, use, creation
C. Control, custody, use
D. Possession, custody, control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Data that falls under the purview of an eDiscovery request is that which is in the possession, custody, or control of the organization. Although this is an easy concept in a traditional data center, it can be difficult to distinguish who actually possesses and controls the data in a cloud environment due to multitenancy and resource pooling. Although these options provide similar-sounding terms, they are ultimately incorrect.

QUESTION 13
Which of the following threat types involves the sending of commands or arbitrary data through input fields in an application in an attempt to get that code executed as part of normal processing?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An injection attack is where a malicious actor will send commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. This can trick an application into exposing data that is not intended or authorized to be exposed, or it could potentially allow an attacker to gain insight into configurations or security controls. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes.

QUESTION 14
With a cloud service category where the cloud customer is responsible for deploying all services, systems, and components needed for their applications, which of the following storage types are MOST likely to be available to them?

A. Structured and hierarchical
B. Volume and object
C. Volume and database
D. Structured and unstructured

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 15
Which of the following roles would be responsible for managing memberships in federations and the use and integration of federated services?

A. Inter-cloud provider
B. Cloud service business manager
C. Cloud service administrator
D. Cloud service integrator

Correct Answer: A

Section: (none)
Explanation

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

QUESTION 16
Which data state would be most likely to use TLS as a protection mechanism?

A. Data in use
B. Data at rest
C. Archived

D.
Data in transit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
TLS would be used with data in transit, when packets are exchanged between clients or services and sent across a network. During the data-in-use state, the data is already protected via a technology such as TLS as it is exchanged over the network and then relies on other technologies such as digital signatures for protection while being used. The data-at-rest state primarily uses encryption for stored file objects. Archived data would be the same as data at rest.

QUESTION 17
You are working for a cloud service provider and receive an eDiscovery order pertaining to one of your customers.

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

A. Take a shapshot of the virtual machines
B. Escrow the encryption keys
C. Copy the data
D. Notify the customer

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 18
If a cloud computing customer wishes to guarantee that a minimum level of resources will always be available, which of the following set of services would compromise the reservation?

D.

A. Memory and networking
B. CPU and software
C. CPU and storage
   CPU and memory

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources. A reservation pertains to memory and CPU resources. Under the concept of a reservation, memory and CPU are the guaranteed resources, but storage and networking are not included even though they are core components of cloud computing. Software would be out of scope for a guarantee and doesn't really pertain to the concept.

QUESTION 19
Which of the following threat types can occur when baselines are not appropriately applied or when unauthorized changes are made?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner. This can be due to a shortcoming in security baselines or configurations, unauthorized changes to system configurations, or a failure to patch and upgrade systems as the vendor releases security patches. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, allowing spoofing for malware or phishing attacks. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data.

D.

QUESTION 20

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

A. Power feeds
B. Chillers
C. Network circuits
Generators

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Chillers and cooling systems are internal to a data center and its operations, and as such they are considered an internal redundancy. Power feeds, network circuits, and generators are all external to a data center and provide utility services to them, which makes them an external redundancy.

QUESTION 21

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 to see the results of the commands, it does open other ways to compromise an application. Missing functionlevel access control exists where an application only checks for authorization during the initial login process and does not further validate with each

D.
function call. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes.

QUESTION 22
With finite resources available within a cloud, even the largest cloud providers will at times need to determine which customers will receive additional resources first.

What is the term associated with this determination?

A. Weighting
B. Prioritization
C. Shares
D. Scoring

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Shares are used within a cloud environment to prioritize resource allocation when customer requests exceed the available resources. Cloud providers utilize shares by assigning a priority score to each customer and allocating resources to those with the highest scores first. Scoring is a component of shares that determines the actual order in which to allocate resources. Neither weighting nor prioritization is the correct term in this case.

QUESTION 23
In order to comply with regulatory requirements, which of the following secure erasure methods would be available to a cloud customer using volume storage within the IaaS service model?

A. Demagnetizing
B. Shredding
C. Degaussing
D. Cryptographic erasure

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 24
Where is a DLP solution generally installed when utilized for monitoring data in use?

A. Application server

B. Database server
C. Network perimeter
D. User's client

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To monitor data in use, the DLP solution's optimal location would be on the user's client or workstation, where the data would be used or processed, and where it would be most vulnerable to access or exposure. The network perimeter is most appropriate for data in transit, and an application server would serve as middle stage between data at rest and data in use, but is a less correct answer than a user's client. A database server would be an example of a location appropriate for monitoring data at rest.

QUESTION 25
Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers. Especially within a public cloud model, it is not possible or practical for a cloud provider to alter its services for specific customer demands. Resource pooling and virtualization within a cloud environment would be the same for all customers, and would not impact certifications that a cloud provider might be willing to pursue. Regulations would form the basis for certification problems and would be a reason for a cloud provider to pursue specific certifications to meet customer requirements.

QUESTION 26
Which phase of the cloud data lifecycle would be the MOST appropriate for the use of DLP technologies to protect the data?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
During the share phase, data is allowed to leave the application for consumption by other vendors, systems, or services. At this point, as the data is leaving the security controls of the application, the use of DLP technologies is appropriate to control how the data is used or to force expiration. During the use, create, and store phases, traditional security controls are available and are more appropriate because the data is still internal to the application.

QUESTION 27
During which phase of the cloud data lifecycle is it possible for the classification of data to change?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The create phase encompasses any time data is created, imported, or modified. With any change in the content or value of data, the classification may also change. It must be continually reevaluated to ensure proper security. During the use, share, and archive phases, the data is not modified in any way, so the original classification is still relevant.

QUESTION 28
If a key feature of cloud computing that your organization desires is the ability to scale and expand without limit or concern about available resources, which cloud deployment model would you MOST likely be considering?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Public clouds, such as AWS and Azure, are massive systems run by major corporations, and they account for a significant share of Internet traffic and services. They are always expanding, offer enormous resources to customers, and are the least likely to run into resource constraints compared to the other deployment models. Private clouds would likely have the resources available for specific uses and could not be assumed to have a large pool of resources available for expansion. A community cloud would have the same issues as a private cloud, being targeted to similar organizations. A hybrid cloud, because it spans multiple clouds, would not fit the bill either, without the use of individual cloud models.

QUESTION 29
What is a serious complication an organization faces from the compliance perspective with international operations?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, which often may not be clearly applicable or may be in contention with each other. These requirements can involve the location of the users and the type of data they enter into systems, the laws governing the organization that owns the application and any regulatory requirements they may have, and finally the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which may be multiple jurisdictions as well. Different certifications would not come into play as a challenge because the major IT and data center certifications are international and would apply to any cloud provider. Different capabilities and different operational procedures would be mitigated by the organization's selection of a cloud provider and would not be a challenge if an appropriate provider was chosen, regardless of location.

QUESTION 30
ISO/IEC has established international standards for many aspects of computing and any processes or procedures related to information technology.

Which ISO/IEC standard has been established to provide a framework for handling eDiscovery processes?

A. ISO/IEC 27001
B. ISO/IEC 27002
C. ISO/IEC 27040
D. ISO/IEC 27050

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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, including the identification, preservation, collection, processing, review, analysis, and the final production of the requested data archive. ISO/IEC 27001 is a general security specification for an information security management system. ISO/IEC 27002 gives best practice recommendations for information security management. ISO/IEC 27040 is focused on the security of storage systems.

QUESTION 31
If a company needed to guarantee through contract and SLAs that a cloud provider would always have available sufficient resources to start their services and provide a certain level of provisioning, what would the contract need to refer to?

A. Limit
B. Reservation
C. AssuranceD. Guarantee

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources. A limit refers to the enforcement of a maximum level of resources that can be consumed by or allocated to a cloud customer, service, or system. Both guarantee and assurance are terms that sound similar to reservation, but they are not correct choices.

QUESTION 32
Many aspects and features of cloud computing can make eDiscovery compliance more difficult or costly.

Which aspect of cloud computing would be the MOST complicating factor?

A. Measured service
B. Broad network access
C. Multitenancy
D. Portability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With multitenancy, multiple customers share the same physical hardware and systems. With the nature of a cloud environment and how it writes data across diverse systems that are shared by others, the process of eDiscovery becomes much more complicated. Administrators cannot pull physical drives or easily isolate which data to capture. They not only have to focus on which data they need to collect, while ensuring they find all of it, but they also have to make sure that other data is not accidently collected and exposed along with it. Measured service is the aspect of a cloud where customers only pay for the services they are actually using, and for the duration of their use. Portability refers to the ease with which an application or service can be moved among different cloud providers. Broad network access refers to the nature of cloud services being accessed via the public Internet, either with or without secure tunneling technologies. None of these concepts would pertain to eDiscovery.

QUESTION 33
A crucial decision any company must make is in regard to where it hosts the data systems it depends on. A debate exists as to whether it's best to lease space in a data center or build your own data center--and now with cloud computing, whether to purchase resources within a cloud.

What is the biggest advantage to leasing space in a data center versus procuring cloud services?

A. Regulations
B. Control
C. Security
D. Costs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When leasing space in a data center versus utilizing cloud services, a customer has a much greater control over its systems and services, from both the hardware/ software perspective and the operational management perspective. Costs, regulations, and security are all prime considerations regardless of the hosting type selected. Although regulations will be the same in either hosting solution, in most instances, costs and security will be greater factors with leased space.

QUESTION 34
Which of the following systems is used to employ a variety of different techniques to discover and alert on threats and potential threats to systems and networks?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An intrusion detection system (IDS) is implemented to watch network traffic and operations, using predefined criteria or signatures, and alert administrators if anything suspect is found. An intrusion prevention system (IPS) is similar to an IDS but actually takes action against suspect traffic, whereas an IDS just alerts when it finds anything suspect. A firewall works at the network level and only takes into account IP addresses, ports, and protocols; it does not inspect the traffic for patterns or content. A web application firewall (WAF) works at the application layer and provides additional security via proxying, filtering service requests, or blocking based on additional factors such as the client and requests.

QUESTION 35

Which of the following is not a risk management framework?

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

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:
Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe. The rest are not.

QUESTION 36
In order to ensure ongoing compliance with regulatory requirements, which phase of the cloud data lifecycle must be tested regularly?

A. Archive
B. Share
C. Store
D. Destroy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In order to ensure compliance with regulations, it is important for an organization to regularly test the restorability of archived data. As technologies change and older systems are deprecated, the risk rises for an organization to lose the ability to restore data from the format in which it is stored. With the destroy, store, and share phases, the currently used technologies will be sufficient for an organization's needs in an ongoing basis, so the risk that is elevated with archived data is not present.

QUESTION 37
Which of the following threat types involves leveraging a user's browser to send untrusted data to be executed with legitimate access via the user's valid credentials?

A. Injection
B. Missing function-level access control

C. Cross-site scripting
D. Cross-site request forgery

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 perhaps the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with their own access and permissions, allowing the attacker to redirect the user's web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.

QUESTION 38
Digital investigations have adopted many of the same methodologies and protocols as other types of criminal or scientific inquiries.

What term pertains to the application of scientific norms and protocols to digital investigations?

A. Scientific
B. Investigative
C. Methodological
D. Forensics

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Forensics refers to the application of scientific methods and protocols to the investigation of crimes. Although forensics has traditionally been applied to well-known criminal proceedings and investigations, the term equally applies to digital investigations and methods. Although the other answers provide similar-sounding terms and ideas, none is the appropriate answer in this case.

QUESTION 39
Within a federated identity system, which entity accepts tokens from the identity provider?

A. Assertion manager
B. Servicing party
C. Proxy party
D. Relying party

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The relying party is attached to the application or service that a user is trying to access, and it accepts authentication tokens from the user's own identity provider in order to facilitate authentication and access. The other terms provided are all associated with federated systems, but none is the correct choice in this case.

QUESTION 40
Different types of audits are intended for different audiences, such as internal, external, regulatory, and so on.

Which of the following audits are considered "restricted use" versus being for a more broad audience?

A. SOC Type 2
B. SOC Type 1
C. SOC Type 3
D. SAS-70

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 41
Although host-based and network-based IDSs perform similar functions and have similar capabilities, which of the following is an advantage of a network-based IDS over a host-based IDS, assuming all capabilities are equal?

A. Segregated from host systems
B. Network access
C. Scalability
D. External to system patching

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 42
DNSSEC was designed to add a layer of security to the DNS protocol.

Which type of attack was the DNSSEC extension designed to mitigate?

A. Account hijacking
B. Snooping
C. Spoofing
D. Data exposure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DNSSEC is an extension to the regular DNS protocol that utilizes digital signing of DNS query results, which can be verified to come from an authoritative source. This verification mitigates the ability for a rogue DNS server to be used to spoof query results and to direct users to malicious sites. DNSSEC provides for the verification of the integrity of DNS queries. It does not provide any protection from snooping or data exposure. Although it may help lessen account hijacking by preventing users from being directed to rogue sites, it cannot by itself eliminate the possibility.

QUESTION 43
Which aspect of cloud computing pertains to cloud customers only paying for the resources and services they actually use?

A. Metered service
B. Measured billing
C. Metered billing
D. Measured service

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Measured service is the aspect of cloud computing that pertains to cloud services and resources being billed in a metered way, based only on the level of consumption and duration of the cloud customer. Although they sound similar to the correct answer, none of the other choices is the actual cloud terminology.

QUESTION 44
Many of the traditional concepts of systems and services for a traditional data center also apply to the cloud. Both are built around key computing concepts.

Which of the following compromise the two facets of computing?

A. CPU and software
B. CPU and storage
C. CPU and memory
D. Memory and networking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The CPU and memory resources of an environment together comprise its "computing" resources. Cloud environments, especially public clouds, are enormous pools of resources for computing and are typically divided among a large number of customers with constantly changing needs and demands. Although storage and networking are core components of a cloud environment, they do not comprise its computing core. Software, much like within a traditional data center, is highly subjective based on the application, system, service, or cloud computing model used; however, it is not one of the core cloud components.

QUESTION 45
With a cloud service category where the cloud customer is provided a full application framework into which to deploy their code and services, which storage types are MOST likely to be available to them?

A. Structured and unstructured
B. Structured and hierarchical
C. Volume and database
D. Volume and object

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The question is describing the Platform as a Service (PaaS) cloud offering, and as such, structured and unstructured storage types will be available to the customer. Volume and object are storage types associated with IaaS, and although the other answers present similar-sounding storage types, they are a mix of real and fake names.

QUESTION 46
Firewalls are used to provide network security throughout an enterprise and to control what information can be accessed--and to a certain extent, through what means.

Which of the following is NOT something that firewalls are concerned with?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Firewalls work at the network level and control traffic based on the source, destination, protocol, and ports. Whether or not the traffic is encrypted is not a factor with firewalls and their decisions about routing traffic. Firewalls work primarily with IP addresses, ports, and protocols.

QUESTION 47
Within an IaaS implementation, which of the following would NOT be a metric used to quantify service charges for the cloud customer?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Within IaaS, where the cloud customer is responsible for everything beyond the physical network, the number of users on a system would not be a factor in billing or service charges. The core cloud services for IaaS are based on the memory, storage, and CPU requirements of the cloud customer. Because the cloud customer with IaaS is responsible for its own images and deployments, these components comprise the basis of its cloud provisioning and measured services billing.

QUESTION 48
Many different common threats exist against web-exposed services and applications. One attack involves attempting to leverage input fields to execute queries in a nested fashion that is unintended by the developers.

What type of attack is this?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. This can trick an application into exposing data that is not intended or authorized to be exposed, or it can potentially allow an attacker to gain insight into configurations or security controls. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes.

QUESTION 49
For service provisioning and support, what is the ideal amount of interaction between a cloud customer and cloud provider?

A. Half
B. Full
C. Minimal
D. Depends on the contract

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The goal with any cloud-hosting setup is for the cloud customer to be able to perform most or all its functions for service provisioning and configuration without any need for support from or interaction with the cloud provider beyond the automated tools provided. To fulfill the tenants of on-demand self-service, required interaction with the cloud provider--either half time, full time, or a commensurate amount of time based on the contract--would be in opposition to a cloud's intended use. As such, these answers are incorrect.

QUESTION 50
What does a cloud customer purchase or obtain from a cloud provider?

A. Services
B. Hosting
C. Servers
D. Customers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
No matter what form they come in, "services" are obtained or purchased by a cloud customer from a cloud service provider. Services can come in many forms-virtual machines, network configurations, hosting setups, and software access, just to name a few. Hosting and servers--or, with a cloud, more appropriately virtual machines--are just two examples of "services" that a customer would purchase from a cloud provider. "Customers" would never be a service that's purchased.

QUESTION 51
Which phase of the cloud data lifecycle represents the first instance where security controls can be implemented?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The store phase occurs immediately after the create phase, and as data is committed to storage structures, the first opportunity for security controls to be implemented is realized. During the create phase, the data is not yet part of a system where security controls can be applied, and although the use and share phases also entail the application of security controls, they are not the first phase where the process occurs.

QUESTION 52
You were recently hired as a project manager at a major university to implement cloud services for the academic and administrative systems. Because the load and demand for services at a university are very cyclical in nature, commensurate with the academic calendar, which of the following aspects of cloud computing would NOT be a primary benefit to you?

A. Measured service
B. Broad network access
C. Resource pooling
D. On-demand self-service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Broad network access to cloud services, although it is an integral aspect of cloud computing, would not being a specific benefit to an organization with cyclical business needs. The other options would allow for lower costs during periods of low usage as well as provide the ability to expand services quickly and easily when needed for peak periods. Measured service allows a cloud customer to only use the resources it needs at the time, and resource pooling allows a cloud customer to access resources as needed. On-demand self-service enables the cloud customer to change its provisioned resources on its own, without the need to interact with the staff from the cloud provider.

QUESTION 53
Which cloud deployment model is MOST likely to offer free or very cheap services to users?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Public clouds offer services to anyone, regardless of affiliation, and are the most likely to offer free services to users. Examples of public clouds with free services include iCloud, Dropbox, and OneDrive. Private cloud models are designed for specific customers and for their needs, and would not offer services to the public at large, for free or otherwise. A community cloud is specific to a group of similar organizations and would not offer free or widely available public services. A hybrid cloud model would not fit the specifics of the question.

QUESTION 54
Where is a DLP solution generally installed when utilized for monitoring data in transit?

A. Network perimeter
B. Database server
C. Application server
D. Web server

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 55
With IaaS, what is responsible for handling the security and control over the volume storage space?

A. Management plane
B. Operating system
C. Application
D. Hypervisor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Volume storage is allocated via a LUN to a system and then treated the same as any traditional storage. The operating system is responsible for formatting and securing volume storage as well as controlling all access to it. Applications, although they may use volume storage and have permissions to write to it, are not responsible for its formatting and security. Both a hypervisor and the management plane are outside of an individual system and are not responsible for managing the files and storage within that system.

QUESTION 56
Configurations and policies for a system can come from a variety of sources and take a variety of formats. Which concept pertains to the application of a set of configurations and policies that is applied to all systems or a class of systems?

A. Hardening
B. Leveling
C. Baselines
D. Standards

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 57
Which of the following tasks within a SaaS environment would NOT be something the cloud customer would be responsible for?

A. Authentication mechanism
B. Branding
C. Training
D. User access

Correct Answer: A **Section:**
(none) Explanation

Explanation/Reference:
Explanation:
The authentication mechanisms and implementations are the responsibility of the cloud provider because they are core components of the application platform and service. Within a SaaS implementation, the cloud customer will provision user access, deploy branding to the application interface (typically), and provide or procure training for its users.

QUESTION 58
An SLA contains the official requirements for contract performance and satisfaction between the cloud provider and cloud customer.

Which of the following would NOT be a component with measurable metrics and requirements as part of an SLA?
A. Network B.
Users
C. Memory
D. CPU

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Dealing with users or user access would not be an appropriate item for inclusion in an SLA specifically. However, user access and user experience would be covered indirectly through other metrics. Memory, CPU, and network resources are all typically included within an SLA for availability and response times when dealing with any incidents.

QUESTION 59
Within a federated identity system, which of the following would you be MOST likely to use for sending information for consumption by a relying party?

A. XML
B. HTML
C. WS-Federation
D. SAML

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 60
Which data state would be most likely to use digital signatures as a security protection mechanism?

A. Data in use
B. Data in transit
C. Archived
D. Data at rest

Correct Answer: A **Section: (none) Explanation**

Explanation/Reference:
Explanation:

During the data-in-use state, the information has already been accessed from storage and transmitted to the service, so reliance on a technology such as digital signatures is imperative to ensure security and complement the security methods used during previous states. Data in transit relies on technologies such as TLS to encrypt network transmission of packets for security. Data at rest primarily uses encryption for stored file objects. Archived data would be the same as data at rest.

QUESTION 61
There is a large gap between the privacy laws of the United States and those of the European Union. Bridging this gap is necessary for American companies to do business with European companies and in European markets in many situations, as the American companies are required to comply with the stricter requirements.

Which US program was designed to help companies overcome these differences?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 62
Audits are either done based on the status of a system or application at a specific time or done as a study over a period of time that takes into account changes and processes.

Which of the following pairs matches an audit type that is done over time, along with the minimum span of time necessary for it?

A. SOC Type 2, one year
B. SOC Type 1, one year

C. SOC Type 2, one month
D. SOC Type 2, six months

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 63
With software-defined networking (SDN), which two types of network operations are segregated to allow for granularity and delegation of administrative access and functions?

A. Filtering and forwarding
B. Filtering and firewalling
C. Firewalling and forwarding
D. Forwarding and protocol

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With SDN, the filtering and forwarding capabilities and administration are separated. This allows the cloud provider to build interfaces and management tools for administrative delegation of filtering configuration, without having to allow direct access to underlying network equipment. Firewalling and protocols are both terms related to networks, but they are not components SDN is concerned with.

QUESTION 64
Along with humidity, temperature is crucial to a data center for optimal operations and protection of equipment.
Which of the following is the optimal temperature range as set by ASHRAE?

A. 69.8 to 86.0 degrees Fahrenheit (21 to 30 degrees Celsius)
B. 51.8 to 66.2 degrees Fahrenheit (11 to 19 degrees Celsius)
C. 64.4 to 80.6 degrees Fahrenheit (18 to 27 degrees Celsius)

D. 44.6 to 60.8 degrees Fahrenheit (7 to 16 degrees Celsius)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) recommends 64.4 to 80.6 degrees Fahrenheit (or 18 to 27 degrees Celsius) as the optimal temperature range for data centers. None of these options is the recommendation from ASHRAE.

QUESTION 65
Which of the following statements best describes a Type 1 hypervisor?

A. The hypervisor software runs within an operating system tied to the hardware.
B. The hypervisor software runs as a client on a server and needs an external service to administer it.
C. The hypervisor software runs on top of an application layer.
D. The hypervisor software runs directly on “bare metal” without an intermediary.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 66
Which cloud storage type resembles a virtual hard drive and can be utilized in the same manner and with the same type of features and capabilities?

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Volume storage is allocated and mounted as a virtual hard drive within IaaS implementations, and it can be maintained and used the same way a traditional file system can. Object storage uses a flat structure on remote services that is accessed via opaque descriptors, structured storage resembles database storage, and unstructured storage is used to hold auxiliary files in conjunction with applications hosted within a PaaS implementation.

QUESTION 67
Which aspect of SaaS will alleviate much of the time and energy organizations spend on compliance (specifically baselines)?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 68
Many tools and technologies are available for securing or monitoring data in transit within a data center, whether it is a traditional data center or a cloud.

Which of the following is NOT a technology for securing data in transit?

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
DNSSEC is an extension of the normal DNS protocol that enables a system to verify the integrity of a DNS query resolution by signing it from the authoritative source and verifying the signing chain. It is not used for securing data transmissions or exchanges. HTTPS is the most common method for securing web service and data calls within a cloud, and TLS is the current standard for encrypting HTTPS traffic. VPNs are widely used for securing data transmissions and service access.

QUESTION 69
With a federated identity system, where would a user perform their authentication when requesting services or application access?

A. Cloud provider
B. The application
C. Their home organization
D. Third-party authentication system

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 70
Where is an XML firewall most commonly and effectively deployed in the environment?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
An XML firewall is most commonly deployed in line between the firewall and application server to validate XML code before it reaches the application. An XML firewall is intended to validate XML before it reaches the application. Placing the XML firewall between the presentation and application layers, between the firewall and IPS, or between the application and data layers would not serve the intended purpose.

QUESTION 71
Modern web service systems are designed for high availability and resiliency. Which concept pertains to the ability to detect problems within a system, environment, or application and programmatically invoke redundant systems or processes for mitigation?

A. Elasticity
B. Redundancy
C. Fault tolerance
D. Automation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Fault tolerance allows a system to continue functioning, even with degraded performance, if portions of it fail or degrade, without the entire system or service being taken down. It can detect problems within a service and invoke compensating systems or functions to keep functionality going. Although redundancy is similar to fault tolerance, it is more focused on having additional copies of systems available, either active or passive, that can take up services if one system goes down. Elasticity pertains to the ability of a system to resize to meet demands, but it is not focused on system failures. Automation, and its role in maintaining large systems with minimal intervention, is not directly related to fault tolerance.

QUESTION 72
On large distributed systems with pooled resources, cloud computing relies on extensive orchestration to maintain the environment and the constant provisioning of resources.

Which of the following is crucial to the orchestration and automation of networking resources within a cloud?

A. DNSSEC
B. DNS

C. DCOM
D. DHCP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Dynamic Host Configuration Protocol (DHCP) automatically configures network settings for a host so that these settings do not need to be configured on the host statically. Given the rapid and programmatic provisioning of resources within a cloud environment, this capability is crucial to cloud operations. Both DNS and its security-integrity extension DNSSEC provide name resolution to IP addresses, but neither is used for the configuration of network settings on a host. DCOM refers to the Distributed Component Object Model, which was developed by Microsoft as a means to request services across a network, and is not used for network configurations at all.

QUESTION 73
BCDR strategies do not typically involve the entire operations of an organization, but only those deemed critical to their business.

Which concept pertains to the amount of services that need to be recovered to meet BCDR objectives?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the determined level of operations necessary during a BCDR situation. The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. SRE is provided as an erroneous response.

QUESTION 74
During the course of an audit, which of the following would NOT be an input into the control requirements used as part of a gap analysis.

A. Contractual requirements
B. Regulations
C. Vendor recommendations
D. Corporate policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Vendor recommendations would not be pertinent to the gap analysis after an audit. Although vendor recommendations will typically play a role in the development of corporate policies or contractual requirements, they are not required. Regulations, corporate policy, and contractual requirements all determine the expected or mandated controls in place on a system.

QUESTION 75
The GAPP framework was developed through a joint effort between the major Canadian and American professional accounting associations in order to assist their members with managing and preventing risks to the privacy of their data and customers.

Which of the following is the meaning of GAPP?

A. General accounting personal privacy
B. Generally accepted privacy practices
C. Generally accepted privacy principles
D. General accounting privacy policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which protocol operates at the network layer and provides for full point-to-point encryption of all communications and transmissions?

A. IPSec
B. VPN

C. SSL
D. TLS

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 77
When data discovery is undertaken, three main approaches or strategies are commonly used to determine what the type of data, its format, and composition are for the purposes of classification.

Which of the following is NOT one of the three main approaches to data discovery?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 78
There are many situations when testing a BCDR plan is appropriate or mandated.

Which of the following would not be a necessary time to test a BCDR plan?

A. After software updates
B. After regulatory changes
C. After major configuration changes
D. Annually

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Regulatory changes by themselves would not trigger a need for new testing of a BCDR plan. Any changes necessary for regulatory compliance would be accomplished through configuration changes or software updates, which in turn would then trigger the necessary new testing. Annual testing is crucial to any BCDR plan. Also, any time major configuration changes or software updates are done, the plan should be evaluated and tested to ensure it is still valid and complete.

QUESTION 79
Key maintenance and security are paramount within a cloud environment due to the widespread use of encryption for both data and transmissions.

Which of the following key-management systems would provide the most robust control over and ownership of the key-management processes for the cloud customer?

A. Remote key management service
B. Local key management service
C. Client key management service

D. Internal key management service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A remote key management system resides away from the cloud environment and is owned and controlled by the cloud customer. With the use of a remote service, the cloud customer can avoid being locked into a proprietary system from the cloud provider, but also must ensure that service is compatible with the services offered by the cloud provider. A local key management system resides on the actual servers using the keys, which does not provide optimal security or control over them. Both the terms internal key management service and client key management service are provided as distractors.

QUESTION 80
Security is a critical yet often overlooked consideration for BCDR planning.

At which stage of the planning process should security be involved?

A. Scope definition
B. Requirements gathering
C. Analysis
D. Risk assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Defining the scope of the plan is the very first step in the overall process. Security should be included from the very earliest stages and throughout the entire process. Bringing in security at a later stage can lead to additional costs and time delays to compensate for gaps in planning. Risk assessment, requirements gathering, and analysis are all later steps in the process, and adding in security at any of those points can potentially cause increased costs and time delays.

QUESTION 81
Which type of testing uses the same strategies and toolsets that hackers would use?

A. Static
B. Malicious

C. Penetration
D. Dynamic

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 82
Which of the following statements about Type 1 hypervisors is true?

A. The hardware vendor and software vendor are different.
B. The hardware vendor and software vendor are the same
C. The hardware vendor provides an open platform for software vendors.
D. The hardware vendor and software vendor should always be different for the sake of security.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With a Type 1 hypervisor, the management software and hardware are tightly tied together and provided by the same vendor on a closed platform. This allows for optimal security, performance, and support. The other answers are all incorrect descriptions of a Type 1 hypervisor.

QUESTION 83
Which format is the most commonly used standard for exchanging information within a federated identity system?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security Assertion Markup Language (SAML) is the most common data format for information exchange within a federated identity system. It is used to transmit and exchange authentication and authorization data.XML is similar to SAML, but it's used for general-purpose data encoding and labeling and is not used for the exchange of authentication and authorization data in the way that SAML is for federated systems. JSON is used similarly to XML, as a text-based data exchange format that typically uses attribute-value pairings, but it's not used for authentication and authorization exchange. HTML is used only for encoding web pages for web browsers and is not used for data exchange--and certainly not in a federated system.

QUESTION 84
Which ITIL component is focused on anticipating predictable problems and ensuring that configurations and operations are in place to prevent these problems from ever occurring?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Problem management is focused on identifying and mitigating known problems and deficiencies before they are able to occur, as well as on minimizing the impact of incidents that cannot be prevented. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Configuration management tracks and maintains detailed information about all IT components within an organization.

QUESTION 85
Which of the following areas of responsibility would be shared between the cloud customer and cloud provider within the Software as a Service (SaaS) category?

A. Data
B. Governance

C. Application
D. Physical

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 86
When a system needs to be exposed to the public Internet, what type of secure system would be used to perform only the desired operations?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 87
With the rapid emergence of cloud computing, very few regulations were in place that pertained to it specifically, and organizations often had to resort to using a collection of regulations that were not specific to cloud in order to drive audits and policies.

Which standard from the ISO/IEC was designed specifically for cloud computing?

A. ISO/IEC 27001
B. ISO/IEC 19889
C. ISO/IEC 27001:2015
D. ISO/IEC 27018

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 88
Which of the following is NOT considered a type of data loss?

A. Data corruption
B. Stolen by hackers
C. Accidental deletion
D. Lost or destroyed encryption keys

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 89
Which of the following jurisdictions lacks a comprehensive national policy on data privacy and the protection of personally identifiable information (PII)?

A. European Union
B. Asian-Pacific Economic Cooperation

C. United States
D. Russia

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The United States has a myriad of regulations focused on specific types of data, such as healthcare and financial, but lacks an overall comprehensive privacy law on the national level. The European Union, the Asian-Pacific Economic Cooperation, and Russia all have national privacy protections and regulations for the handling the PII data of their citizens.

QUESTION 90
Which component of ITIL involves planning for the restoration of services after an unexpected outage or incident?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 91
Which component of ITIL pertains to planning, coordinating, executing, and validating changes and rollouts to production environments?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Release management involves planning, coordinating, executing, and validating changes and rollouts to the production environment. Change management is a higher-level component than release management and also involves stakeholder and management approval, rather than specifically focusing the actual release itself. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

QUESTION 92

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

Tokenization

B. Encryption
C. Anonymization
D. Masking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Anonymization is a type of masking, where indirect identifiers are removed from a data set to prevent the mapping back of data to an individual. Although masking refers to the overall approach of covering sensitive data, anonymization is the best answer here because it is more specific to exactly what is being asked. Tokenization involves the replacement of sensitive data with a key value that can be matched back to the real value. However, it is not focused on indirect identifiers or preventing the matching to an individual. Encryption refers to the overall process of protecting data via key pairs and protecting confidentiality.

QUESTION 93
Because cloud providers will not give detailed information out about their infrastructures and practices to the general public, they will often use established auditing reports to ensure public trust, where the reputation of the auditors serves for assurance.

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

A. SOC 2
B. SAS-70
C. SOC 3
D. SOC 1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A.
SOC Type 3 audit reports are very similar to SOC Type 2, with the exception that they are intended for general release and public audiences.SAS-70 audits have been deprecated. SOC Type 1 audit reports have a narrow scope and are intended for very limited release, whereas SOC Type 2 audit reports are intended for wider audiences but not general release.

QUESTION 94
Which of the following concepts is NOT one of the core components to an encryption system architecture?

Software
B. Network
C. Keys
D. Data

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The network utilized is not one of the key components of an encryption system architecture. In fact, a network is not even required for encryption systems or the processing and protection of data. The data, software used for the encryption engine itself, and the keys used to implement the encryption are all core components of an encryption system architecture.

QUESTION 95
For optimal security, trust zones are used for network segmentation and isolation. They allow for the separation of various systems and tiers, each with its own security level.

Which of the following is typically used to allow administrative personnel access to trust zones?

A. IPSec
B. SSH
C. VPN
D. TLS

Correct Answer: C
Section: (none)
Explanation

A.

Explanation/Reference:

Explanation:

Virtual private networks (VPNs) are used to provide administrative personnel with secure communication channels through security systems and into trust zones. They allow staff who perform system administration tasks to have access to ports and systems that are not allowed from the public Internet. IPSec is an encryption protocol for point-to-point communications at the network level, and may be used within a trust zone but not to give access into a trust zone. TLS enables encryption of communications between systems and services and would likely be used to secure the VPN communications, but it does not represent the overall concept being asked for in the question. SSH allows for secure shell access to systems, but not for general access into trust zones.

QUESTION 96

Which of the following is NOT a major regulatory framework?

A. PCI DSS
B. HIPAA
C. SOX
D. FIPS 140-2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FIPS 140-2 is a United States certification standard for cryptographic modules, and it provides guidance and requirements for their use based on the requirements of the data classification. However, these are not actual regulatory requirements. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS) are all major regulatory frameworks either by law or specific to an industry.

QUESTION 97
As part of the auditing process, getting a report on the deviations between intended configurations and actual policy is often crucial for an organization.

What term pertains to the process of generating such a report?

A. Deficiencies
B. Findings
C. Gap analysis
D. Errors

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The gap analysis determines if there are any differences between the actual configurations in use on systems and the policies that govern what the configurations are expected or mandated to be. The other terms provided are all similar to the correct answer ("findings" in particular is often used to articulate deviations in configurations), but gap analysis is the official term used.

QUESTION 98
An audit scope statement defines the limits and outcomes from an audit.

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

A. Reports
B. Certification
C. Billing
D. Exclusions

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 99
What concept and operational process must be spelled out clearly, as far as roles and responsibilities go, between the cloud provider and cloud customer for the mitigation of any problems or security events?

A. Incident response
B. Problem management
C. Change management
D. Conflict response

Correct Answer: A **Section:**
(none) Explanation

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

QUESTION 100
Your new CISO is placing increased importance and focus on regulatory compliance as your applications and systems move into cloud environments.

Which of the following would NOT be a major focus of yours as you develop a project plan to focus on regulatory compliance?

A. Data in transit
B. Data in use
C. Data at rest
D. Data custodian

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The jurisdictions where data is being stored, processed, or consumed are the ones that dictate the regulatory frameworks and compliance requirements, regardless of who the data owner or custodian might be. The other concepts for protecting data would all play a prominent role in regulatory compliance with a move to the cloud environment. Each concept needs to be evaluated based on the new configurations as well as any potential changes in jurisdiction or requirements introduced with the move to a cloud.

QUESTION 101
Cloud systems are increasingly used for BCDR solutions for organizations.

What aspect of cloud computing makes their use for BCDR the most attractive?

A. On-demand self-service
B. Measured service
C. Portability
D. Broad network access

Correct Answer: B
Section: (none)
Explanation

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

and although this too would be important for BCDR situations, it is not the best answer because it does not address costs or the biggest benefits to an organization.

QUESTION 102
What's a potential problem when object storage versus volume storage is used within IaaS for application use and dependency?

A. Object storage is only optimized for small files.
B. Object storage is its own system, and data consistency depends on replication.
C. Object storage may have availability issues.
D. Object storage is dependent on access control from the host server.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 103
Many aspects of cloud computing bring enormous benefits over a traditional data center, but also introduce new challenges unique to cloud computing.

Which of the following aspects of cloud computing makes appropriate data classification of high importance?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

With multitenancy, where different cloud customers all share the same physical systems and networks, data classification becomes even more important to ensure that the appropriate security controls are applied immediately to prevent any potential leakage or exposure to other customers. Portability refers to the ability to move easily from one cloud provider to another. Interoperability refers to the ability to reuse components and services for different uses. Reversibility refers to the ability of the cloud customer to quickly and completely remove all data and services from a cloud provider and to verify the removal.

QUESTION 104
Without the extensive funds of a large corporation, a small-sized company could gain considerable and cost-effective services for which of the following concepts by moving to a cloud environment?

A. Regulatory
B. Security
C. Testing
D. Development

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cloud environments, regardless of the specific deployment model used, have extensive and robust security controls in place, especially in regard to physical and infrastructure security. A small company can leverage the extensive security controls and monitoring provided by a cloud provider, which they would unlikely ever be able to afford on their own. Moving to a cloud would not result in any gains for development and testing because these areas require the same rigor regardless of where deployment and hosting occur. Regulatory compliance in a cloud would not be a gain for an organization because it would likely result in additional oversight and auditing as well as require the organization to adapt to a new environment.

QUESTION 105
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.

Which concept pertains to the amount of data and services needed to reach the predetermined level of operations?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the predetermined level of operations necessary during a BCDR situation. The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. SRE is provided as an erroneous response.

QUESTION 106
Which of the following is NOT a commonly used communications method within cloud environments to secure data in transit?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DNSSEC is used as a security extension to DNS lookup queries in order to ensure the authenticity and authoritativeness of hostname resolutions, in order to prevent spoofing and redirection of traffic. Although it is a very important concept to be employed for security practices, it is not used to secure or encrypt data transmissions. HTTPS is the most commonly used security mechanism for data communications between clients and websites and web services. IPSec is less commonly used, but is also intended to secure communications between servers. VPN is commonly used to secure traffic into a network area or subnet for developers and administrative users.

QUESTION 107
Which crucial aspect of cloud computing can be most threatened by insecure APIs?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cloud environments depend heavily on API calls for management and automation. Any vulnerability with the APIs can cause significant risk and exposure to all tenants of the cloud environment. Resource pooling and elasticity could both be impacted by insecure APIs, as both require automation and orchestration to operate properly, but automation is the better answer here. Redundancy would not be directly impacted by insecure APIs.

QUESTION 108
The WS-Security standards are built around all of the following standards except which one?

A. SAML
B. WDSL
C. XML
D. SOAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The WS-Security specifications, as well as the WS-Federation system, are built upon XML, WDSL, and SOAP. SAML is a very similar protocol that is used as an alternative to WS.XML, WDSL, and SOAP are all integral to the WS-Security specifications.

QUESTION 109
Which protocol, as a part of TLS, handles negotiating and establishing a connection between two parties?

A. Record
B. Binding
C. NegotiationD. Handshake

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 110
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.

Which concept pertains to the required amount of time to restore services to the predetermined level?
A. RPO
B. RSL
C. RTO
D. SRE

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the predetermined level of operations necessary during a BCDR situation. SRE is provided as an erroneous response.

QUESTION 111
Your company is in the planning stages of moving applications that have large data sets to a cloud environment.

What strategy for data removal would be the MOST appropriate for you to recommend if costs and speed are primary considerations?

A. Shredding
B. Media destruction
C. Crypthographic erasure
D. Overwriting

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cryptographic erasure involves having the data encrypted, typically as a matter of standard operations, and then rendering the data useless and unreadable by destroying the encryption keys for it. It represents a very cheap and immediate way to destroy data, and it works in all environments. With a cloud environment and multitenancy, media destruction or the physical destruction of storage devices, including shredding, would not be possible. Depending on the environment, overwriting may or may not be possible, but cryptographic erasure is the best answer because it is always an available option and is very quick to implement.

QUESTION 112
Which of the following is a management role, versus a technical role, as it pertains to data management and oversight?

A. Data owner
B. Data processor
C. Database administrator
D. Data custodian

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 113
IRM solutions allow an organization to place different restrictions on data usage than would otherwise be possible through traditional security controls.

Which of the following controls would be possible with IRM that would not with traditional security controls?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 114

B.

Which data protection strategy would be useful for a situation where the ability to remove sensitive data from a set is needed, but a requirement to retain the ability to map back to the original values is also present?

A. Masking
Tokenization
C. Encryption
D. Anonymization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Tokenization involves the replacement of sensitive data fields with key or token values, which can ultimately be mapped back to the original, sensitive data values. Masking refers to the overall approach to covering sensitive data, and anonymization is a type of masking, where indirect identifiers are removed from a data set to prevent the mapping back of data to an individual. Encryption refers to the overall process of protecting data via key pairs and protecting confidentiality.

QUESTION 115
A comprehensive BCDR plan will encapsulate many or most of the traditional concerns of operating a system in any data center.

However, what is one consideration that is often overlooked with the formulation of a BCDR plan?

A. Availability of staff
B. Capacity at the BCDR site
C. Restoration of services
D. Change management processes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

C.
BCDR planning tends to focus so much on the failing over of services in the case of a disaster that recovery back to primary hosting after the disaster is often overlooked. In many instances, this can be just as complex a process as failing over, if not more so. Availability of staff, capacity at the BCDR site, and change management processes are typically integral to BCDR plans and are common components of them.

QUESTION 116
Which of the following is NOT one of the components of multifactor authentication?

A. Something the user knows
B. Something the user has
Something the user sends
D. Something the user is

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Multifactor authentication systems are composed of something the user knows, has, and/or is, not something the user sends. Multifactor authentication commonly uses something that a user knows, has, and/or is (such as biometrics or features).

QUESTION 117
Above and beyond general regulations for data privacy and protection, certain types of data are subjected to more rigorous regulations and oversight.

Which of the following is not a regulatory framework for more sensitive or specialized data?

A. FIPS 140-2
B. FedRAMP
C. PCI DSS
D. HIPAA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

D.

Explanation:

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

QUESTION 118

Which data sanitation method is also commonly referred to as "zeroing"?

A. Overwriting
B. Nullification
C. Blanking
D. Deleting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The zeroing of data--or the writing of null values or arbitrary data to ensure deletion has been fully completed--is officially referred to as overwriting. Nullification, deleting, and blanking are provided as distractor terms.

QUESTION 119
What is the concept of isolating an application from the underlying operating system for testing purposes?

A. Abstracting
B. Application virtualization
C. Hosting
D. Sandboxing

Correct Answer: B **Section: (none) Explanation**

Explanation/Reference:
Explanation:
Application virtualization is a software implementation that allows applications and programs to run in an isolated environment rather than directly interacting with the operating system. Sandboxing refers to segregating information or processes for security or testing purposes, but it's not directly related to isolation from the underlying operating system. Abstracting sounds similar to the correct term but is not pertinent to the question, and hosting is provided as an erroneous answer.

QUESTION 120
Which of the following could be used as a second component of multifactor authentication if a user has an RSA token?

A. Access card
B. USB thumb drive
C. Retina scan
D. RFID

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

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

QUESTION 121
Which of the following is NOT one of the official risk rating categories?

A. Critical
B. Low
C. Catastrophic
D. Minimal

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The official categories of cloud risk ratings are Minimal, Low, Moderate, High, and Critical.

QUESTION 122
SOC Type 1 reports are considered "restricted use," in that they are intended only for limited audiences and purposes.

Which of the following is NOT a population that would be appropriate for a SOC Type 1 report?

A. Current clients
B. Auditors
C. Potential clients
D. The service organization

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 123
Having a reservation in a cloud environment can ensure operations continue in the event of high utilization across the cloud.

Which of the following would NOT be a capability covered by reservations?

A. Performing business operations
B. Starting virtual machines
C. Running applications
D. Auto-scaling

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A reservation will not guarantee auto-scaling is available because it involves the allocation of additional resources beyond what a cloud customer already has provisioned. Reservations will guarantee minimal resources are available to start virtual machines, run applications, and perform normal business operations.

QUESTION 124
What must SOAP rely on for security since it does not provide security as a built-in capability?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for data passing, and it must rely on the encryption of those data packages for security. TLS and SSL (before it was deprecated) represent two commons approaches to using encryption for protection of data transmissions. However, they are only two possible options and do not encapsulate the overall concept the question is looking for. Tokenization, which involves the replacement of sensitive data with opaque values, would not be appropriate for use with SOAP because the actual data is needed by the services.

QUESTION 125
With a federated identity system, what does the identity provider send information to after a successful authentication?

A. Relying party
B. Service originator
C. Service relay
D. Service relay

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Upon successful authentication, the identity provider sends an assertion with appropriate attributes to the relying party to grant access and assign appropriate roles to the user. The other terms provided are similar sounding to the correct term but are not actual components of a federated system.

QUESTION 126
Which of the following technologies is NOT commonly used for accessing systems and services in a cloud environment in a secure manner?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A keyboard-video-mouse (KVM) system is commonly used for directly accessing server terminals in a data center. It is not a method that would be possible within a cloud environment, primarily due to the use virtualized systems, but also because only the cloud provider's staff would be allowed the physical access to hardware systems that's provided by a KVM. Hypertext Transfer Protocol Secure (HTTPS), virtual private network (VPN), and Transport Layer Security (TLS) are all technologies and protocols that are widely used with cloud implementations for secure access to systems and services.

QUESTION 127
Which component of ITIL involves handling anything that can impact services for either internal or public users?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation
Incident management is focused on limiting the impact of disruptions to an organization's services or operations, as well as returning their state to full operational status as soon as possible. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur. Deployment management is a subcomponent of change management and is where the actual code or configuration change is put into place. Change management involves the processes and procedures that allow an organization to make changes to its IT systems and services in a controlled manner.

QUESTION 128
Which protocol, as a part of TLS, handles the actual secure communications and transmission of data?

A. Negotiation
B. Handshake
C. Transfer
D. Record

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 129
Which of the following terms is NOT a commonly used category of risk acceptance?

A. Moderate
B. Critical
C. Minimal
D. Accepted

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation
Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

QUESTION 130
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: (none)
Explanation

Explanation/Reference:
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 131
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: (none)
Explanation

Explanation/Reference:
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 132
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: (none)
Explanation

Explanation/Reference:
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 133
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: (none)
Explanation

Explanation/Reference:
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 134
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: (none)
Explanation

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

QUESTION 135
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: (none)
Explanation

Explanation/Reference:
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 136
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: (none)
Explanation

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

QUESTION 137
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: (none)
Explanation

Explanation/Reference:
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 138
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: (none)

Explanation

Explanation/Reference:
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 139
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: (none)
Explanation

Explanation/Reference:
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 140
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:**
(none) Explanation

Explanation/Reference:
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 141
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: (none)
Explanation

Explanation/Reference:
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 142
Which of the following is NOT a component of access control?

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

Correct Answer: B **Section:**
(none) Explanation

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

QUESTION 143
What concept does the A represent within the DREAD model?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 144
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: (none)
Explanation

Explanation/Reference:
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 145
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: (none)
Explanation

Explanation/Reference:
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 146
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: (none)
Explanation

Explanation/Reference:
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 147
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: (none)
Explanation

Explanation/Reference:
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 148
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: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 149
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: (none)
Explanation
Explanation/Reference:
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 150
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: (none)
Explanation

Explanation/Reference:
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 151
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: (none)
Explanation

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

QUESTION 152
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: (none)
Explanation

Explanation/Reference:
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 153
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

Section: (none)
Explanation

Explanation/Reference:

Explanation:

Correct Answer: B
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 154
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: (none)
Explanation

Explanation/Reference:
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 155
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

Section: (none)
Explanation

Explanation/Reference:

Explanation:

Correct Answer: B
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 156
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: (none)
Explanation

Explanation/Reference:
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 157
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

Section: (none)
Explanation

Explanation/Reference:

Explanation:

Correct Answer: C
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 158
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: (none)
Explanation

Explanation/Reference:
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 159
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
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

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 160
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: (none)
Explanation

Explanation/Reference:
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 161
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: (none)
Explanation
Explanation/Reference:
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 162
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: (none)
Explanation

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

QUESTION 163
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: (none)
Explanation

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

QUESTION 164
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: (none)
Explanation

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

QUESTION 165
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: (none)
Explanation

Explanation/Reference:

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 166
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: (none)
Explanation

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

QUESTION 167
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: (none)
Explanation

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

QUESTION 168
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: (none)
Explanation

Explanation/Reference:
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 169
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: (none)
Explanation

Explanation/Reference:
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 170
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: (none)
Explanation

Explanation/Reference:
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 171
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: (none)
Explanation

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

QUESTION 172
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: (none)
Explanation

Explanation/Reference:
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 173
When using a PaaS solution, what is the capability provided to the customer?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
According to “The NIST Definition of Cloud Computing,” in PaaS, “the capability provided to the consumer is to deploy onto the cloud infrastructure consumercreated 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 174
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: (none)
Explanation

Explanation/Reference:

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 175
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: (none)
Explanation

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

QUESTION 176
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:**
(none) Explanation

Explanation/Reference:
Explanation:
Layered defense calls for a diverse approach to security.

QUESTION 177

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: (none)
Explanation

Explanation/Reference:
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 tendollar 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 178
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: (none)
Explanation

Explanation/Reference:
Explanation:
The following groups form the key roles and functions associated with cloud computing. They do not constitute an exhaustive list but highlight the main roles and functions within cloud computing:
- Cloud customer: An individual or entity that utilizes or subscribes to cloud based services or resources.
- CSP: A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations or individuals, usually for a fee; otherwise known to clients “as a service.

- Cloud backup service provider: A third-party entity that manages and holds operational responsibilities for cloud-based data backup services and solutions to customers from a central data center.
- CSB: Typically a third-party entity or company that looks to extend or enhance value to multiple customers of cloud-based services through relationships with multiple CSPs. It acts as a liaison between cloud services customers and CSPs, selecting the best provider for each customer and monitoring the services. The CSB can be utilized as a “middleman” to broker the best deal and customize services to the customer’s requirements. May also resell cloud services. - Cloud service auditor: Third-party organization that verifies attainment of SLAs.

QUESTION 179
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: (none)
Explanation

Explanation/Reference:

QUESTION 180
Which of the following is considered a physical control?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 181
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: (none)
Explanation

Explanation/Reference:
Explanation:
Homomorphic encryption hopes to achieve that goal; the other options are terms that have almost nothing to do with encryption.

QUESTION 182
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: (none)
Explanation

Explanation/Reference:
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 183

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: (none)
Explanation

Explanation/Reference:
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 184
Tokenization requires two distinct _____ .

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 185
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: (none)
Explanation

Explanation/Reference:
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 186
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: (none)
Explanation

Explanation/Reference:
Explanation:
Confidential recipes unique to the organization are trade secrets. The other answers listed are answers to other questions.

QUESTION 187
Every security program and process should have which of the following?

A. Severe penalties
B. Multifactor authenticationC. Foundational policy
D. Homomorphic encryption

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
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 188
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: (none)
Explanation

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

QUESTION 189
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: (none)
Explanation

Explanation/Reference:
Explanation:
All the elements except adjudication need to be addressed in each policy. Adjudication is not an element of policy.

QUESTION 190
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: (none)
Explanation

Explanation/Reference:
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 191
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: (none)
Explanation

Explanation/Reference:
Explanation:
AES is an encryption standard. Link encryption is a method for protecting communications traffic. One-time pads are an encryption method.

QUESTION 192
Data labels could include all the following, except:

A. Multifactor authentication
B. Access restrictions
C. Confidentiality level
D. Distribution limitations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All the others might be included in data labels, but multifactor authentication is a procedure used for access control, not a label.

QUESTION 193
In the cloud motif, the data owner is usually:

A. The cloud provider
B. In another jurisdiction
C. The cloud customer
D. The cloud access security broker

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 194
The goals of DLP solution implementation include all of the following, except:

A. Elasticity
B. Policy enforcement
C. Data discovery
D. Loss of mitigation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DLP does not have anything to do with elasticity, which is the capability of the environment to scale up or down according to demand. All the rest are goals of DLP implementations.

QUESTION 195
What is the intellectual property protection for a useful manufacturing innovation?
A. Trademark
B. Copyright
C. patent
D. Trade secret

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Patents protect processes (as well as inventions, new plantlife, and decorative patterns). The other answers listed are answers to other questions.

QUESTION 196
The most pragmatic option for data disposal in the cloud is which of the following?

A. Cryptoshredding
B. Overwriting
C. Cold fusion
D. Melting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
We don't have physical ownership, control, or even access to the devices holding the data, so physical destruction, including melting, is not an option. Overwriting is a possibility, but it is complicated by the difficulty of locating all the sectors and storage areas that might have contained our data, and by the likelihood that constant backups in the cloud increase the chance we'll miss something as it's being overwritten. Cryptoshredding is the only reasonable alternative. Cold fusion is a red herring.

QUESTION 197
In the cloud motif, the data processor is usually:

A. The cloud customer
B. The cloud provider
C. The cloud access security broker
D. The party that assigns access rights

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In legal terms, when "data processor" is defined, it refers to anyone who stores, handles, moves, or manipulates data on behalf of the data owner or controller. In the cloud computing realm, this is the cloud provider.

QUESTION 198
What is the intellectual property protection for the tangible expression of a creative idea?

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

Correct Answer: B **Section:**
(none) Explanation

Explanation/Reference:
Explanation:
Copyrights are protected tangible expressions of creative works. The other answers listed are answers to subsequent questions.

QUESTION 199
The goals of SIEM solution implementation include all of the following, except:

A. Dashboarding
B. Performance enhancement
C. Trend analysis
D. Centralization of log streams

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SIEM does not intend to provide any enhancement of performance; in fact, a SIEM solution may decrease performance because of additional overhead. All the rest are goals of SIEM implementations.

QUESTION 200
Data masking can be used to provide all of the following functionality, except:

A. Secure remote access
B. test data in sandboxed environments
C. Authentication of privileged users
D. Enforcing least privilege

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 201
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:

A. Tokenization
B. Masking
C. Data discovery
D. Obfuscation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Data discovery is a term used to describe the process of identifying information according to specific traits or categories. The rest are all methods for obscuring data.

QUESTION 202
DLP solutions can aid in deterring loss due to which of the following?
A. Power failure
B. Performance
C. Bad policy
D. Malicious disclosure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

DLP tools can identify outbound traffic that violates the organization's policies. DLP will not protect against losses due to performance issues or power failures. The DLP solution must be configured according to the organization's policies, so bad policies will attenuate the effectiveness of DLP tools, not the other way around.

QUESTION 203
All the following are data analytics modes, except:

A. Datamining
B. Agile business intelligence
C. Refractory iterations
D. Real-time analytics

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 204
What are the U.S. State Department controls on technology exports known as?

A. DRM
B. ITAR
C. EAR
D. EAL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ITAR is a Department of State program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Digital rights management tools are used for protecting electronic processing of intellectual property.

QUESTION 205
When crafting plans and policies for data archiving, we should consider all of the following, except:

A. The backup process
B. Immediacy of the technology
C. Archive location
D. The format of the data

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All of these things should be considered when creating data archival policies, except option D, which is a nonsense term.

QUESTION 206
DLP solutions can aid in deterring loss due to which of the following?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 207
DLP can be combined with what other security technology to enhance data controls?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 208
The goals of SIEM solution implementation include all of the following, except:

A. Dashboarding
B. Performance enhancement
C. Trend analysis
D. Centralization of log streams

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SIEM does not intend to provide any enhancement of performance; in fact, a SIEM solution may decrease performance because of additional overhead. All the rest are goals of SIEM implementations.

QUESTION 209
What is the cloud service model in which the customer is responsible for administration of the OS?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In IaaS, the cloud provider only owns the hardware and supplies the utilities. The customer is responsible for the OS, programs, and data. In PaaS and SaaS, the provider also owns the OS. There is no QaaS. That is a red herring.

QUESTION 210
All of the following are techniques to enhance the portability of cloud data, in order to minimize the potential of vendor lock-in except:

A. Ensure there are no physical limitations to moving
B. Use DRM and DLP solutions widely throughout the cloud operation
C. Ensure favorable contract terms to support portability
D. Avoid proprietary data formats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DRM and DLP are used for increased authentication/access control and egress monitoring, respectively, and would actually decrease portability instead of enhancing it.

QUESTION 211
Hardening the operating system refers to all of the following except:

A. Limiting administrator access
B. Closing unused ports
C. Removing antimalware agents
D. Removing unnecessary services and libraries

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Removing antimalware agents. Hardening the operating system means making it more secure. Limiting administrator access, closing unused ports, and removing unnecessary services and libraries all have the potential to make an OS more secure. But removing antimalware agents would actually make the system less secure. If anything, antimalware agents should be added, not removed.

QUESTION 212
Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider?

A. SOC 1 Type 1
B. SOC 2 Type 2
C. SOC 3
D. SOC 1 Type 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The SOC 3 is the least detailed, so the provider is not concerned about revealing it. The SOC 1 Types 1 and 2 are about financial reporting, and not relevant. The SOC 2 Type 2 is much more detailed and will most likely be kept closely held by the provider.

QUESTION 213
The cloud customer's trust in the cloud provider can be enhanced by all of the following except:

A. SLAs
B. Shared administration
C. Audits
D. real-time video surveillance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Video surveillance will not provide meaningful information and will not enhance trust. All the others will do it.

QUESTION 214

As a result of scandals involving publicly traded corporations such as Enron, WorldCom, and Adelphi, Congress passed legislation known as:

A. SOX
B. HIPAA
C. FERPA
D. GLBA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sarbanes-Oxley was a direct response to corporate scandals. FERPA is related to education. GLBA is about the financial industry. HIPAA is about health care.

QUESTION 215
In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?

A. HIPAA
B. The contract
C. Statutes
D. Security control matrix

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable. The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

QUESTION 216
The application normative framework is best described as which of the following?
A. A superset of the ONF

B. A stand-alone framework for storing security practices for the ONF
C. The complete ONF
D. A subnet of the ONF

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Remember, there is a one-to-many ratio of ONF to ANF; each organization has one ONF and many ANFs (one for each application in the organization). Therefore, the ANF is a subset of the ONF.

QUESTION 217
Deviations from the baseline should be investigated and _____.

A. Revealed
B. Documented
C. Encouraged
D. Enforced

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 218
Which of the following best describes the Organizational Normative Framework (ONF)?

A. A set of application security, and best practices, catalogued and leveraged by the organization
B. A container for components of an application’s security, best practices catalogued and leveraged by the organization
C. A framework of containers for some of the components of application security, best practices, catalogued and leveraged by the organization
D. A framework of containers for all components of application security, best practices, catalogued and leveraged by the organization.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Option B is incorrect, because it refers to a specific applications security elements, meaning it is about an ANF, not the ONF. C is true, but not as complete as D, making D the better choice. C suggests that the framework contains only “some” of the components, which is why B (which describes “all” components) is better

QUESTION 219
A UPS should have enough power to last how long?

A. One day
B. 12 hours
C. Long enough for graceful shutdown
D. 10 minutes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Team-building has nothing to do with SAST; all the rest of the answers are characteristics of SAST.

QUESTION 220
Which of the following best describes the purpose and scope of ISO/IEC 27034-1?

A. Describes international privacy standards for cloud computing
B. Serves as a newer replacement for NIST 800-52 r4
C. Provides on overview of network and infrastructure security designed to secure cloud applications.
D. Provides an overview of application security that introduces definitive concepts, principles, and processes involved in application security.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
Which of the following best describes SAML?

A. A standard used for directory synchronization
B. A standard for developing secure application management logistics
C. A standard for exchanging usernames and passwords across devices.
D. A standards for exchanging authentication and authorization data between security domains.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222
Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like:

A. Ransomware
B. Syn floods
C. XSS and SQL injection
D. Password cracking

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 223
APIs are defined as which of the following?

A. A set of protocols, and tools for building software applications to access a web-based software application or tool
B. A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or tool

C. A set of standards for building software applications to access a web-based software application or tool
D. A set of routines and tools for building software applications to access web-based software applications

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 224
Which of the following best describes data masking?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All of these answers are actually correct, but A is the best answer, because it is the most general, includes the others, and is therefore the optimum choice. This is a good example of the type of question that can appear on the actual exam.

QUESTION 225
Which of the following best describes a sandbox?

A. An isolated space where untested code and experimentation can safely occur separate from the production environment.
B. A space where you can safely execute malicious code to see what it does.
C. An isolated space where transactions are protected from malicious software
D. An isolated space where untested code and experimentation can safely occur within the production environment.

Correct Answer: A

Section: (none)
Explanation
Explanation/Reference:
Explanation:
Options C and B are also correct, but A is more general and incorporates them both. D is incorrect, because sandboxing does not take place in the production environment.

QUESTION 226
A localized incident or disaster can be addressed in a cost-effective manner by using which of the following?

A. UPS
B. Generators
C. Joint operating agreements
D. Strict adherence to applicable regulations

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Joint operating agreements can provide nearby relocation sites so that a disruption limited to the organization's own facility and campus can be addressed at a different facility and campus. UPS and generators are not limited to serving needs for localized causes. Regulations do not promote cost savings and are not often the immediate concern during BC/DR activities.

QUESTION 227
In addition to battery backup, a UPS can offer which capability?

A. Breach alert
B. Confidentiality
C. Communication redundancy
D. Line conditioning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
A UPS can provide line conditioning, adjusting power so that it is optimized for the devices it serves and smoothing any power fluctuations; it does not offer any of the other listed functions.

QUESTION 228
For performance purposes, OS monitoring should include all of the following except:

A. Disk space
B. Disk I/O usage
C. CPU usage
D. Print spooling

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Print spooling is not a metric for system performance; all the rest are.

QUESTION 229
Identity and access management (IAM) is a security discipline that ensures which of the following?

A. That all users are properly authorized
B. That the right individual gets access to the right resources at the right time for the right reasons.
C. That all users are properly authenticated
D. That unauthorized users will get access to the right resources at the right time for the right reasons

Correct Answer: B **Section: (none)**
Explanation

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

QUESTION 230
Maintenance mode requires all of these actions except:

A. Remove all active production instances

B. Ensure logging continues
C. Initiate enhanced security controls
D. Prevent new logins

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
While the other answers are all steps in moving from normal operations to maintenance mode, we do not necessarily initiate any enhanced security controls.

QUESTION 231
What is one of the reasons a baseline might be changed?

A. Numerous change requests
B. To reduce redundancy
C. Natural disaster
D. Power fluctuation

Correct Answer: A **Section: (none) Explanation**

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

QUESTION 232
In a federated identity arrangement using a trusted third-party model, who is the identity provider and who is the relying party?

A. The users of the various organizations within the federations within the federation/a CASB
B. Each member organization/a trusted third party
C. Each member organization/each member organization
D. A contracted third party/the various member organizations of the federation

Correct Answer: D

Section: (none)
Explanation
Explanation/Reference:
Explanation:
In a trusted third-party model of federation, each member organization outsources the review and approval task to a third party they all trust. This makes the third party the identifier (it issues and manages identities for all users in all organizations in the federation), and the various member organizations are the relying parties (the resource providers that share resources based on approval from the third party).

QUESTION 233
Database activity monitoring (DAM) can be:

A. Host-based or network-based
B. Server-based or client-based
C. Used in the place of encryption
D. Used in place of data masking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
We don't use DAM in place of encryption or masking; DAM augments these options without replacing them. We don't usually think of the database interaction as client-server, so A is the best answer.

QUESTION 234
The BC/DR kit should include all of the following except:

A. Annotated asset inventory
B. Flashlight
C. Hard drives
D. Documentation equipment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
While hard drives may be useful in the kit (for instance, if they store BC/DR data such as inventory lists, baselines, and patches), they are not necessarily required. All the other items should be included.

QUESTION 235
The baseline should cover which of the following?

A. Data breach alerting and reporting
B. All regulatory compliance requirements
C. As many systems throughout the organization as possible
D. A process for version control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The more systems that be included in the baseline, the more cost-effective and scalable the baseline is. The baseline does not deal with breaches or version control; those are the provinces of the security office and CMB, respectively. Regulatory compliance might (and usually will) go beyond the baseline and involve systems, processes, and personnel that are not subject to the baseline.

QUESTION 236
Which of the following roles is responsible for creating cloud components and the testing and validation of services?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 237

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

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

Correct Answer: D **Section: (none) Explanation**

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

QUESTION 238
A data custodian is responsible for which of the following?

A. Data context
B. Data content
C. The safe custody, transport, storage of the data, and implementation of business rules
D. Logging access and alerts

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:
Explanation:
A data custodian is responsible for the safe custody, transport, and storage of data, and the implementation of business roles.

QUESTION 239
Which of the following is the least challenging with regard to eDiscovery in the cloud?

A. Identifying roles such as data owner, controller and processor
B. Decentralization of data storage
C. Forensic analysis
D. Complexities of International law

Correct Answer: C
Section: (none)

Explanation
Explanation/Reference:
Explanation:
Forensic analysis is the least challenging of the answers provided as it refers to the analysis of data once it is obtained. The challenges revolve around obtaining the data for analysis due to the complexities of international law, the decentralization of data storage or difficulty knowing where to look, and identifying the data owner, controller, and processor.

QUESTION 240
What is the Cloud Security Alliance Cloud Controls Matrix (CCM)?

A. A set of software development life cycle requirements for cloud service providers
B. An inventory of cloud services security controls that are arranged into a hierarchy of security domains
C. An inventory of cloud service security controls that are arranged into separate security domains
D. A set of regulatory requirements for cloud service providers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The CSA CCM is an inventory of cloud service security controls that are arranged into separate security domains, not a hierarchy.

QUESTION 241
Which of the following is a valid risk management metric?

A. KPI
B. KRI
C. SOC
D. SLA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

KRI stands for key risk indicator. KRIs are the red flags if you will in the world of risk management. When these change, they indicate something is amiss and should be looked at quickly to determine if the change is minor or indicative of something important.

QUESTION 242
Which of the following is the best example of a key component of regulated PII?

A. Audit rights of subcontractors
B. Items that should be implemented
C. PCI DSS
D. Mandatory breach reporting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Mandatory breach reporting is the best example of regulated PII components. The rest are generally considered components of contractual PII.

QUESTION 243
Which of the following components are part of what a CCSP should review when looking at contracting with a cloud service provider?

A. Redundant uplink grafts
B. Background checks for the provider's personnel
C. The physical layout of the datacenter
D. Use of subcontractors

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The use of subcontractors can add risk to the supply chain and should be considered; trusting the provider's management of their vendors and suppliers (including subcontractors) is important to trusting the provider. Conversely, the customer is not likely to be allowed to review the physical design of the datacenter (or, indeed, even know the exact location of the datacenter) or the personnel security specifics for the provider's staff. "Redundant uplink grafts" is a nonsense term used as a distractor.

QUESTION 244
Which of the following is not a way to manage risk?

A. Transferring
B. Accepting
C. Mitigating D. Enveloping

Correct Answer: D **Section: (none) Explanation**

Explanation/Reference:
Explanation:
Enveloping is a nonsense term, unrelated to risk management. The rest are not.

QUESTION 245
Which of the following terms is not associated with cloud forensics?

A. eDiscovery
B. Chain of custody
C. Analysis
D. Plausibility

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:
Explanation:
Plausibility, here, is a distractor and not specifically relevant to cloud forensics.

QUESTION 246
Which is the lowest level of the CSA STAR program?

A. Attestation
B. Self-assessment
C. Hybridization
D. Continuous monitoring

Correct Answer: B

Section: (none)
Explanation
Explanation/Reference:
Explanation:
The lowest level is Level 1, which is self-assessment, Level 2 is an external third-party attestation, and Level 3 is a continuous-monitoring program. Hybridization does not exist as part of the CSA STAR program.

QUESTION 247
Which of the following is the primary purpose of an SOC 3 report?

A. HIPAA compliance
B. Absolute assurances
C. Seal of approval
D. Compliance with PCI/DSS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The SOC 3 report is more of an attestation than a full evaluation of controls associated with a service provider.

QUESTION 248
Which of the following is not an example of a highly regulated environment?

A. Financial services
B. Healthcare
C. Public companies
D. Wholesale or distribution

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Wholesalers or distributors are generally not regulated, although the products they sell may be.

QUESTION 249
Which of the following methods of addressing risk is most associated with insurance?

A. Mitigation
B. Transference
C. Avoidance
D. Acceptance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Avoidance halts the business process, mitigation entails using controls to reduce risk, acceptance involves taking on the risk, and transference usually involves insurance.

QUESTION 250
Legal controls refer to which of the following?

A. ISO 27001
B. PCI DSS
C. NIST 800-53r4
D. Controls designed to comply with laws and regulations related to the cloud environment

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 251
Which of the following best describes a cloud carrier?

A. The intermediary who provides connectivity and transport of cloud providers and cloud consumers
B. A person or entity responsible for making a cloud service available to consumers
C. The person or entity responsible for transporting data across the Internet
D. The person or entity responsible for keeping cloud services running for customers

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:
Explanation:
A cloud carrier is the intermediary who provides connectivity and transport of cloud services between cloud providers and cloud customers.

QUESTION 252
Gap analysis is performed for what reason?

A. To begin the benchmarking process
B. To assure proper accounting practices are being used
C. To provide assurances to cloud customers
D. To ensure all controls are in place and working properly

Correct Answer: A
Section: (none) Explanation

Explanation/Reference: Explanation:
The primary purpose of the gap analysis is to begin the benchmarking process against risk and security standards and frameworks.

QUESTION 253

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

A. ISO 31000:2009
B. ISO 27017
C. NIST 800-92
D. HIPAA

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 254
Which of the following report is most aligned with financial control audits?

A. SSAE 16
B. SOC 2
C. SOC 1
D. SOC 3

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 255
Which of the following is not a risk management framework?

A. COBIT
B. Hex GBL

C. ISO 31000:2009D. NIST SP 800-37

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 256
Limits for resource utilization can be set at different levels within a cloud environment to ensure that no particular entity can consume a level of resources that impacts other cloud customers.

Which of the following is NOT a unit covered by limits?

A. Hypervisor
B. Cloud customer
C. Virtual machine
D. Service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The hypervisor level, as a backend cloud infrastructure component, is not a unit where limits may be applied to control resource utilization. Limits can be placed at the service, virtual machine, and cloud customer levels within a cloud environment.

QUESTION 257
Which of the following is the dominant driver behind the regulations to which a system or application must adhere?

A. Data source
B. Locality
C. Contract
D. SLA

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The locality--or physical location and jurisdiction where the system or data resides--is the dominant driver of regulations. This may be based on the type of data contained within the application or the way in which the data is used. The contract and SLA both articulate requirements for regulatory compliance and the responsibilities for the cloud provider and cloud customer, but neither artifact defines the actual requirements. Instead, the contract and SLA merely form the official documentation between the cloud provider and cloud customer. The source of the data may place contractual requirements or best practice guidelines on its usage, but ultimately jurisdiction has legal force and greater authority.

QUESTION 258
When using a SaaS solution, what is the capability provided to the customer?

A. To use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited userspecific application configuration settings.
B. To use the consumer's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited userspecific application configuration settings.
C. To use the consumer's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited userspecific application configuration settings.
D. To use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited userspecific application configuration settings.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
According to "The NIST Definition of Cloud Computing," in SaaS, "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or

a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."