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 233
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
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 234
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
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 235
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
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 236
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
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 237
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
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 238
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
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 239
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
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 240
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
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 241
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
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 242
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
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 243
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
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 244
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
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 245
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
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 246
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
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 247