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

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

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

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

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

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

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

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

QUESTION 52

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

A. Remove
B. Monitor
C. Disable
D. Stop

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

QUESTION 53
Which of the following actions will NOT make data part of the "create" phase of the cloud data lifecycle?

A. Modifying metadata
B. Importing data
C. Modifying data
D. Constructing new data

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

QUESTION 54
What are the two protocols that TLS uses?

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

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

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

A. IaaS
B. DaaS
C. SaaS

D. PaaS

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

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

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

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

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

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

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

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

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

Correct Answer: D
Explanation:
Limits are put in place to enforce a maximum on the amount of memory or processing a cloud customer can use. This can be done either on a virtual machine or as a comprehensive whole for a customer, and is meant to ensure that enormous cloud resources cannot be allocated or

consumed by a single host or customer to the detriment of other hosts and customers.

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

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

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

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

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

Correct Answer: B
Explanation:
Federation pertains to authenticating systems between different organizations.

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

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

Correct Answer: A

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

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

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

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

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

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

QUESTION 64
Which of the following represents a prioritization of applications or cloud customers for the allocation of additional requested resources when there is a limitation on available resources?

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

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

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

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

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

QUESTION 66
Which of the following statements accurately describes VLANs?