QUESTION 83
When is a virtual machine susceptible to attacks while a physical server in the same state would not be?

A.   When it is behind a WAF
B.   When it is behind an IPS
C.   When it is not patched
D.   When it is powered off

Correct Answer: D
Explanation:
A virtual machine is ultimately an image file residing a file system. Because of this, even when a virtual machine is "powered off," it is still susceptible to attacks and modification. A physical server that is powered off would not be susceptible to attacks.

QUESTION 84
Which of the following threat types involves an application developer leaving references to internal information and configurations in code that is exposed to the client?

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

Correct Answer: C
Explanation:
An insecure direct object reference occurs when a developer has in their code a reference to something on the application side, such as a database key, the directory structure of the application, configuration information about the hosting system, or any other information that pertains to the workings of the application that should not be exposed to users or the network. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, allowing spoofing for malware of phishing attacks. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data. Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner.

QUESTION 85
Which of the following is the biggest concern or challenge with using encryption?

A.   Dependence on keys
B.   Cipher strength
C.   Efficiency
D.   Protocol standards

Correct Answer: A
Explanation:
No matter what kind of application, system, or hosting model used, encryption is 100 percent dependent on encryption keys. Properly securing the keys and the exchange of them is the biggest and most important challenge of encryption systems.

QUESTION 86
Which of the following would NOT be considered part of resource pooling with an Infrastructure as a Service implementation?

A. Storage
B. Application
C. Mamory
D. CPU

Correct Answer: B
Explanation:
Infrastructure as a Service pools the compute resources for platforms and applications to build upon, including CPU, memory, and storage. Applications are not part of an IaaS offering from the cloud provider.

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

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

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

QUESTION 88
Which of the following roles is responsible for gathering metrics on cloud services and managing cloud deployments and the deployment processes?

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

Correct Answer: D
Explanation:
The cloud service deployment manager is responsible for gathering metrics on cloud services, managing cloud deployments and the deployment process, and defining the environments and processes.

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

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

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

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

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

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

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

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

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

QUESTION 92
What controls the formatting and security settings of a volume storage system within a cloud environment?

A. Management plane
B. SAN host controller
C. Hypervisor
D. Operating system of the host

Correct Answer: D
Explanation:
Once a storage LUN is allocated to a virtual machine, the operating system of that virtual machine will format, manage, and control the file system and security of the data on that LUN.

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

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

Correct Answer: B
Explanation:
Software-defined networking separates the administration of network filtering and network forwarding to allow for distributed administration.

QUESTION 94
From a legal perspective, what is the most important first step after an eDiscovery order has been received by the cloud provider?

A. Notification
B. Key identification
C. Data collection
D. Virtual image snapshots

Correct Answer: A
Explanation:
The contract should include requirements for notification by the cloud provider to the cloud customer upon the receipt of such an order. This serves a few important purposes. First, it keeps communication and trust open between the cloud provider and cloud customers. Second, and more importantly, it allows the cloud customer to potentially challenge the order if they feel they have the grounds or desire to do so.

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

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

Correct Answer: C
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, and especially within a public cloud model, it is not possible or practical for a cloud provider to alter their services for specific customer demands.

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

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

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

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

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

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

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

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

Correct Answer: B
Explanation:
Masking involves replacing specific data within a data set with new values. For example, with credit card fields, as most who have ever purchased anything online can attest, nearly the entire credit card number is masked with a character such as an asterisk, with the last four digits left visible for identification and confirmation.

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

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

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