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

Correct Answer: B
Explanation:
Interoperability is the ease with which one can move or reuse components of an application or service. This is maximized when services are designed without specific dependencies on underlying platforms, operating systems, locations, or cloud providers.

QUESTION 154
Which of the following is a restriction that can be enforced by information rights management (IRM) that is not possible for traditional file system controls?

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

Correct Answer: D
Explanation:
IRM allows an organization to control who can print a set of information. This is not be possible under traditional file system controls, where if a user can read a file, they are able to print it as well.

QUESTION 155
What strategy involves hiding data in a data set to prevent someone from identifying specific individuals based on other data fields present?

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

Correct Answer: A
Explanation:
With data anonymization, data is manipulated in such a way so as to prevent the identification of an individual through various data objects, and is often used in conjunction with other concepts such as masking.

QUESTION 156
What type of security threat is DNSSEC designed to prevent?

A. Account hijacking
B. Snooping
C. Spoofing
D. Injection

Correct Answer: C
Explanation:

DNSSEC is designed to prevent the spoofing and redirection of DNS resolutions to rogue sites.

QUESTION 157
Which European Union directive pertains to personal data privacy and an individual's control over their personal data?

A.   99/9/EC
B.   95/46/EC
C.   2000/1/EC
D.   2013/27001/EC

Correct Answer: B
Explanation:
Directive 95/46/EC is titled "On the protection of individuals with regard to the processing of personal data and on the free movement of such data."

QUESTION 158
Which of the cloud cross-cutting aspects relates to the requirements placed on a system or application by law, policy, or requirements from standards?

A.   regulatory requirements
B.   Auditability
C.   Service-level agreements
D.   Governance

Correct Answer: A
Explanation:
Regulatory requirements are those imposed upon businesses and their operations either by law, regulation, policy, or standards and guidelines. These requirements are specific either to the locality in which the company or application is based or to the specific nature of the data and transactions conducted.

QUESTION 159
Which data point that auditors always desire is very difficult to provide within a cloud environment?

A.   Access policy
B.   Systems architecture
C.   Baselines
D.   Privacy statement

Correct Answer: B
Explanation:
Cloud environments are constantly changing and often span multiple physical locations. A cloud customer is also very unlikely to have knowledge and insight into the underlying systems architecture in a cloud environment. Both of these realities make it very difficult, if not impossible, for an organization to provide a comprehensive systems design document.

QUESTION 160
What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?

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

Correct Answer: B
Explanation:
A bastion host is a server that is fully exposed to the public Internet, but is extremely hardened to prevent attacks and is usually dedicated for a specific application or usage; it is not something that will serve multiple purposes. This singular focus allows for much more stringent security hardening and monitoring.

QUESTION 161
Which security concept is focused on the trustworthiness of data?

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

Correct Answer: A
Explanation:
Integrity is focused on the trustworthiness of data as well as the prevention of unauthorized modification or tampering of it. A prime consideration for maintaining integrity is an emphasis on the change management and configuration management aspects of operations, so that all modifications are predictable, tracked, logged, and verified, whether they are performed by actual human users or systems processes and scripts.

QUESTION 162
Which OSI layer does IPsec operate at?

A. Network
B. transport
C. Application
D. Presentation

Correct Answer: A
Explanation:
A major difference between IPsec and other protocols such as TLS is that IPsec operates at the Internet network layer rather than the application layer, allowing for complete end-to-end encryption of all communications and traffic.

QUESTION 163
Which of the cloud cross-cutting aspects relates to the requirements placed on the cloud provider by the cloud customer for minimum performance standards and requirements that must be met?

A. Regulatory requirements
B. SLAs
C. Auditability

D. Governance

Correct Answer: B
Explanation:
Whereas a contract spells out general terms and costs for services, the SLA is where the real meat of the business relationship and concrete requirements come into play. The SLA spells out in clear terms the minimum requirements for uptime, availability, processes, customer service and support, security controls and requirements, auditing and reporting, and potentially many other areas that define the business relationship and the success of it.

QUESTION 164
Which of the following service capabilities gives the cloud customer the most control over resources and configurations?

A. Desktop
B. Platform
C. Infrastructure
D. Software

Correct Answer: C
Explanation:
The infrastructure service capability gives the cloud customer substantial control in provisioning and configuring resources, including processing, storage, and network resources.

QUESTION 165
What concept does the "I" represent with the STRIDE threat model?

A. Integrity
B. Information disclosure
C. IT security
D. Insider threat

Correct Answer: B
Explanation:
Perhaps the biggest concern for any user is having their personal and sensitive information disclosed by an application. There are many aspects of an application to consider with security and protecting this information, and it is very difficult for any application to fully ensure security from start to finish. The obvious focus is on security within the application itself, as well as protecting and storing the data.

QUESTION 166
At which stage of the BCDR plan creation phase should security be included in discussions?

A. Define scope
B. Analyze
C. Assess risk
D. Gather requirements

Correct Answer: A
Explanation:
Security should be included in discussions from the very first phase when defining the scope. Adding security later is likely to incur additional costs in time and money, or will result in an

incomplete or inadequate plan.

QUESTION 167
Which approach is typically the most efficient method to use for data discovery?

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

Correct Answer: A
Explanation:
Metadata is data about data. It contains information about the type of data, how it is stored and organized, or information about its creation and use.

QUESTION 168
Which of the following features is a main benefit of PaaS over IaaS?

A. Location independence
B. High-availability
C. Physical security requirements
D. Auto-scaling

Correct Answer: D
Explanation:
With PaaS providing a fully configured and managed framework, auto-scaling can be implemented to programmatically adjust resources based on the current demands of the environment.

QUESTION 169
Which audit type has been largely replaced by newer approaches since 2011?

A. SOC Type 1
B. SSAE-16
C. SAS-70
D. SOC Type 2

Correct Answer: C
Explanation:
SAS-70 reports were replaced in 2011 with the SSAE-16 reports throughout the industry.

QUESTION 170
Which of the following can be useful for protecting cloud customers from a denial-of-service (DoS) attack against another customer hosted in the same cloud?

A. Reservations
B. Measured service
C. Limits
D. Shares

Correct Answer: A