# ISC2

## Exam Questions CCSP

Certified Cloud Security Professional

**NEW QUESTION 1**
- (Exam Topic 4)
The cloud customer will have the most control of their data and systems, and the cloud provider will have the least amount of responsibility, in which cloud computing arrangement?

A. IaaS
B. SaaS
C. Community cloud
D. PaaS

**Answer:** A

**Explanation:**
IaaS entails the cloud customer installing and maintaining the OS, programs, and data; PaaS has the customer installing programs and data; in SaaS, the customer only uploads data. In a community cloud, data and device owners are distributed.

**NEW QUESTION 2**
- (Exam Topic 4)
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

**Answer:** A

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

**NEW QUESTION 3**
- (Exam Topic 4)
The WS-Security standards are built around all of the following standards except which one?

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

**Answer:** A

**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.

**NEW QUESTION 4**
- (Exam Topic 4)
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

**Answer:** A

**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.

**NEW QUESTION 5**
- (Exam Topic 4)
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

**Answer:** A

**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.

**NEW QUESTION 6**
- (Exam Topic 4)
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

**Answer:** A

**NEW QUESTION 7**
- (Exam Topic 4)
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

**Answer:** B

**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.

**NEW QUESTION 8**
- (Exam Topic 4)
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

**Answer:** C

**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.

**NEW QUESTION 9**
- (Exam Topic 3)
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

**Answer:** C

**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.

**NEW QUESTION 10**
- (Exam Topic 3)
The European Union is often considered the world leader in regard to the privacy of personal data and has declared privacy to be a "human right."
In what year did the EU first assert this principle?

A. 1995
B. 2000
C. 2010

D. 1999

**Answer:** A

**Explanation:**
SThe EU passed Directive 95/46 EC in 1995, which established data privacy as a human right. The other years listed are incorrect.

**NEW QUESTION 11**
- (Exam Topic 3)
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

**Answer:** A

**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 host-based 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.

**NEW QUESTION 12**
- (Exam Topic 3)
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

**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.

**NEW QUESTION 13**
- (Exam Topic 3)
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

**Answer:** D

**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.

**NEW QUESTION 14**
- (Exam Topic 3)
You just hired an outside developer to modernize some applications with new web services and functionality. In order to implement a comprehensive test platform for validation, the developer needs a data set that resembles a production data set in both size and composition.
In order to accomplish this, what type of masking would you use?

A. Development
B. Replicated
C. Static
D. Dynamic

**Answer:** C

**Explanation:**
Static masking takes a data set and produces a copy of it, but with sensitive data fields masked. This allows for a full data set from production for testing purposes, but without any sensitive data. Dynamic masking works with a live system and is not used to produce a distinct copy. The terms "replicated" and "development" are not types of masking.

**NEW QUESTION 15**
- (Exam Topic 3)
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

**Answer:** C

**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.

**NEW QUESTION 16**
- (Exam Topic 2)
Which OSI layer does IPsec operate at?

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

**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.

**NEW QUESTION 17**
- (Exam Topic 2)
What concept does the "I" represent with the STRIDE threat model?

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

**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.

**NEW QUESTION 18**
- (Exam Topic 2)
Which of the following is NOT a function performed by the handshake protocol of TLS?

A. Key exchange
B. Encryption
C. Negotiation of connection
D. Establish session ID

**Answer:** B

**Explanation:**
The handshake protocol negotiates and establishes the connection as well as handles the key exchange and establishes the session ID. It does not perform the actual encryption of data packets.

**NEW QUESTION 19**
- (Exam Topic 2)
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

**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.

**NEW QUESTION 20**
- (Exam Topic 2)
Which type of controls are the SOC Type 1 reports specifically focused on?

A. Integrity
B. PII
C. Financial
D. Privacy

**Answer:** C

**Explanation:**
SOC Type 1 reports are focused specifically on internal controls as they relate to financial reporting.

**NEW QUESTION 21**
- (Exam Topic 2)
What is an often overlooked concept that is essential to protecting the confidentiality of data?

A. Strong password
B. Training
C. Security controls
D. Policies

**Answer:** B

**Explanation:**
While the main focus of confidentiality revolves around technological requirements or particular security methods, an important and often overlooked aspect of safeguarding data confidentiality is appropriate and comprehensive training for those with access to it. Training should be focused on the safe handling of sensitive information overall, including best practices for network activities as well as physical security of the devices or workstations used to access the application.

**NEW QUESTION 22**
- (Exam Topic 2)
What provides the information to an application to make decisions about the authorization level appropriate when granting access?

A. User
B. Relying party
C. Federation
D. Identity Provider

**Answer:** D

**Explanation:**
Upon successful user authentication, the identity provider gives information about the user to the relying party that it needs to make authorization decisions for granting access as well as the level of access needed.

**NEW QUESTION 23**
- (Exam Topic 2)
Which of the following would be a reason to undertake a BCDR test?

A. Functional change of the application
B. Change in staff
C. User interface overhaul of the application
D. Change in regulations

**Answer:** A

**Explanation:**
Any time a major functional change of an application occurs, a new BCDR test should be done to ensure the overall strategy and process are still applicable and appropriate.

**NEW QUESTION 24**
- (Exam Topic 2)
Which security concept is focused on the trustworthiness of data?

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

**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.

**NEW QUESTION 25**
- (Exam Topic 1)
What is the biggest concern with hosting a key management system outside of the cloud environment?

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

**Answer:** C

**Explanation:**
When a key management system is outside of the cloud environment hosting the application, availability is a primary concern because any access issues with the encryption keys will render the entire application unusable.

**NEW QUESTION 26**
- (Exam Topic 1)
Which of the following attempts to establish an international standard for eDiscovery processes and best practices?

A. ISO/IEC 31000
B. ISO/IEC 27050
C. ISO/IEC 19888
D. ISO/IEC 27001

**Answer:** B

**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: identification, preservation, collection, processing, review, analysis, and the final production of the requested data.

**NEW QUESTION 27**
- (Exam Topic 1)
What type of PII is regulated based on the type of application or per the conditions of the specific hosting agreement?

A. Specific
B. Contractual
C. regulated
D. Jurisdictional

**Answer:** B

**Explanation:**
Contractual PII has specific requirements for the handling of sensitive and personal information, as defined at a contractual level. These specific requirements will typically document the required handling procedures and policies to deal with PII. They may be in specific security controls and configurations, required policies or procedures, or limitations on who may gain authorized access to data and systems.

**NEW QUESTION 28**
- (Exam Topic 1)
Which of the following is not a risk management framework?

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

**Answer:** B

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

**NEW QUESTION 29**
- (Exam Topic 1)
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

**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.

**NEW QUESTION 30**

- (Exam Topic 1)
What is used for local, physical access to hardware within a data center?

A. SSH
B. KVM
C. VPN
D. RDP

**Answer:** B

**Explanation:**
Local, physical access in a data center is done via KVM (keyboard, video, mouse) switches.

**NEW QUESTION 31**

......