Vendor: (ISC)2

Exam Code: CCSP

Exam Name: Certified Cloud Security Professional (CCSP)

Version: DEMO

QUESTION 1
Over time, what is a primary concern for data archiving?

A. Size of archives
B. Format of archives
C. Recoverability
D. Regulatory changes

Answer: C
Explanation:
Over time, maintaining the ability to restore and read archives is a primary concern for data archiving. As technologies change and new systems are brought in, it is imperative for an organization to ensure they are still able to restore and access archives for the duration of the required retention period.

QUESTION 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.

QUESTION 3
Which of the cloud deployment models offers the most control and input to the cloud customer as to how the overall cloud environment is implemented and configured?

A. Public
B. Community
C. Hybrid
D. Private

Answer: D
Explanation:
A private cloud model, and the specific contractual relationships involved, will give a cloud customer the most level of input and control over how the overall cloud environment is designed and implemented. This would be even more so in cases where the private cloud is owned and operated by the same organization that is hosting services within it.

QUESTION 4
What concept does the "D" represent with the STRIDE threat model?

A. Data loss

B. Denial of service
C. Data breach
D. Distributed

Answer: B
Explanation:
Any application can be a possible target of denial-of-service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for non-authenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks.

QUESTION 5
Your boss has tasked your team with getting your legacy systems and applications connected with new cloud-based services that management has decided are crucial to customer service and offerings.

Which role would you be assuming under this directive?

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

Answer: C
Explanation:
The cloud service integrator role is responsible for connecting and integrating existing services and applications with cloud-based 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 user is someone who consumes cloud services. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

QUESTION 6
One of the main components of system audits is the ability to track changes over time and to match these changes with continued compliance and internal processes.

Which aspect of cloud computing makes this particular component more challenging than in a traditional data center?

A. Portability
B. Virtualization
C. Elasticity
D. Resource pooling

Answer: B
Explanation:
Cloud services make exclusive use of virtualization, and systems change over time, including the addition, subtraction, and reimaging of virtual machines. It is extremely unlikely that the exact same virtual machines and images used in a previous audit would still be in use or even available for a later audit, making the tracking of changes over time extremely difficult, or even impossible. Elasticity refers to the ability to add and remove resources from a system or service to meet current demand, and although it plays a factor in making the tracking of virtual machines very

difficult over time, it is not the best answer in this case.
Resource pooling pertains to a cloud environment sharing a large amount of resources between different customers and services. Portability refers to the ability to move systems or services easily between different cloud providers.

QUESTION 7
In the wake of many scandals with major corporations involving fraud and the deception of investors and regulators, which of the following laws was passed to govern accounting and financial records and disclosures?

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

Answer: D
Explanation:
The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and accounting errors.The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy.
The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Safe Harbor program was designed by the US government as a way for American companies to comply with European Union privacy laws.

QUESTION 8
Which one of the following threat types to applications and services involves the sending of requests that are invalid and manipulated through a user's client to execute commands on the application under the user's own credentials?

A. Injection
B. Missing function-level access control
C. Cross-site scripting
D. Cross-site request forgery

Answer: D
Explanation:
A cross-site request forgery (CSRF) attack forces a client that a user has used to authenticate to an application to send forged requests under the user's own credentials to execute commands and requests that the application thinks are coming from a trusted client and user. Although this type of attack cannot be used to steal data directly because the attacker has no way of seeing the results of the commands, it does open other ways to compromise an application. 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 scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes. An injection attack is where a malicious actor sends 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.

QUESTION 9
Which cloud service category would be most ideal for a cloud customer that is developing software to test its applications among multiple hosting providers to determine the best option for

its needs?

A. DaaS
B. PaaS
C. IaaS
D. SaaS

Answer: B
Explanation:
Platform as a Service would allow software developers to quickly and easily deploy their applications among different hosting providers for testing and validation in order to determine the best option. Although IaaS would also be appropriate for hosting applications, it would require too much configuration of application servers and libraries in order to test code. Conversely, PaaS would provide a ready-to-use environment from the onset. DaaS would not be appropriate in any way for software developers to use to deploy applications. IaaS would not be appropriate in this scenario because it would require the developers to also deploy and maintain the operating system images or to contract with another firm to do so. SaaS, being a fully functional software platform, would not be appropriate for deploying applications into.

QUESTION 10
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.

QUESTION 11
In order to prevent cloud customers from potentially consuming enormous amounts of resources within a cloud environment and thus having a negative impact on other customers, what concept is commonly used by a cloud provider?

A. Limit
B. Cap
C. Throttle
D. Reservation

Answer: A
Explanation:
A limit puts a maximum value on the amount of resources that may be consumed by either a system, a service, or a cloud customer. It is commonly used to prevent one entity from consuming

enormous amounts of resources and having an operational impact on other tenants within the same cloud system.
Limits can either be hard or somewhat flexible, meaning a customer can borrow from other customers while still having their actual limit preserved. A reservation is a guarantee to a cloud customer that a certain level of resources will always be available to them, regardless of what operational demands are currently placed on the cloud environment. Both cap and throttle are terms that sound similar to limit, but they are not the correct terms in this case.

QUESTION 12
Where is a DLP solution generally installed when utilized for monitoring data at rest?

A. Network firewall
B. Host system
C. Application server
D. Database server

Answer: B
Explanation:
To monitor data at rest appropriately, the DLP solution would be installed on the host system where the data resides. A database server, in some situations, may be an appropriate answer, but the host system is the best answer because a database server is only one example of where data could reside. An application server processes data and typically sits between the data and presentation zones, and as such, does not store data at rest. A network firewall would be more appropriate for data in transit because it is not a place where data would reside.

QUESTION 13
Which of the following aspects of security is solely the responsibility of the cloud provider?

A. Regulatory compliance
B. Physical security
C. Operating system auditing
D. Personal security of developers

Answer: B
Explanation:
Regardless of the particular cloud service used, physical security of hardware and facilities is always the sole responsibility of the cloud provider. The cloud provider may release information about their physical security policies and procedures to ensure any particular requirements of potential customers will meet their regulatory obligations. Personal security of developers and regulatory compliance are always the responsibility of the cloud customer. Responsibility for operating systems, and the auditing of them, will differ based on the cloud service category used.

QUESTION 14
Humidity levels for a data center are a prime concern for maintaining electrical and computing resources properly as well as ensuring that conditions are optimal for top performance.

Which of the following is the optimal humidity level, as established by ASHRAE?

A. 20 to 40 percent relative humidity
B. 50 to 75 percent relative humidity
C. 40 to 60 percent relative humidity

D. 30 to 50 percent relative humidity

Answer: C
Explanation:
The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) recommends 40 to 60 percent relatively humidity for data centers. None of these options is the recommendation from ASHRAE.

QUESTION 15
Within a SaaS environment, what is the responsibility on the part of the cloud customer in regard to procuring the software used?

A. Maintenance
B. Licensing
C. Development
D. Purchasing

Answer: B
Explanation:
Within a SaaS implementation, the cloud customer licenses the use of the software from the cloud provider because SaaS delivers a fully functional application to the customer. With SaaS, the cloud provider is responsible for the entire software application and any necessary infrastructure to develop, run, and maintain it. The purchasing, development, and maintenance are fully the responsibility of the cloud provider.

QUESTION 16
Implementing baselines on systems would take an enormous amount of time and resources if the staff had to apply them to each server, and over time, it would be almost impossible to keep all the systems in sync on an ongoing basis.

Which of the following is NOT a package that can be used for implementing and maintaining baselines across an enterprise?

A. Puppet
B. SCCM
C. Chef
D. GitHub

Answer: D
Explanation:
GitHub is a software development platform that serves as a code repository and versioning system. It is solely used for software development and would not be appropriate for applying baselines to systems.
Puppet is an open-source configuration management tool that runs on many platforms and can be used to apply and maintain baselines. The Software Center Configuration Manager (SCCM) was developed by Microsoft for managing systems across large groups of servers. Chef is also a system for maintaining large groups of systems throughout an enterprise.

QUESTION 17
From the perspective of compliance, what is the most important consideration when it comes to data center location?

A. Natural disasters
B. Utility access
C. Jurisdiction
D. Personnel access

Answer: C
Explanation:
Jurisdiction will dictate much of the compliance and audit requirements for a data center. Although all the aspects listed are very important to security, from a strict compliance perspective, jurisdiction is the most important. Personnel access, natural disasters, and utility access are all important operational considerations for selecting a data center location, but they are not related to compliance issues like jurisdiction is.

QUESTION 18
Different certifications and standards take different approaches to data center design and operations. Although many traditional approaches use a tiered methodology, which of the following utilizes a macro- level approach to data center design?

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

Answer: A
Explanation:
The Infinity Paradigm of the International Data Center Authority (IDCA) takes a macro-level approach to data center design. The IDCA does not use a specific, focused approach on specific components to achieve tier status. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers.

QUESTION 19
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:
The EU passed Directive 95/46 EC in 1995, which established data privacy as a human right. The other years listed are incorrect.

QUESTION 20

A DLP solution/implementation has three main components.

Which of the following is NOT one of the three main components?

A. Monitoring
B. Enforcement
C. Auditing
D. Discovery and classification

Answer: C
Explanation:
Auditing, which can be supported to varying degrees by DLP solutions, is not a core component of them.
Data loss prevention (DLP) solutions have core components of discovery and classification, enforcement, and monitoring. Discovery and classification are concerned with determining which data should be applied to the DLP policies, and then determining its classification level. Monitoring is concerned with the actual watching of data and how it's used through its various stages. Enforcement is the actual application of policies determined from the discovery stage and then triggered during the monitoring stage.

QUESTION 21
What type of storage structure does object storage employ to maintain files?

A. Directory
B. Hierarchical
C. tree
D. Flat

Answer: D
Explanation:
Object storage uses a flat file system to hold storage objects; it assigns files a key value that is then used to access them, rather than relying on directories or descriptive filenames. Typical storage layouts such as tree, directory, and hierarchical structures are used within volume storage, whereas object storage maintains a flat structure with key values.

QUESTION 22
Which cloud storage type requires special consideration on the part of the cloud customer to ensure they do not program themselves into a vendor lock-in situation?

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

Answer: D
Explanation:
Structured storage is designed, maintained, and implemented by a cloud service provider as part of a PaaS offering. It is specific to that cloud provider and the way they have opted to implement systems, so special care is required to ensure that applications are not designed in a way that will lock the cloud customer into a specific cloud provider with that dependency. Unstructured storage for auxiliary files would not lock a customer into a specific provider. With volume and object storage, because the cloud customer maintains their own systems with IaaS, moving and

replicating to a different cloud provider would be very easy.

QUESTION 23
Which cloud deployment model would be ideal for a group of universities looking to work together, where each university can gain benefits according to its specific needs?

A. Private
B. Public
C. Hybrid
D. Community

Answer: D
Explanation:
A community cloud is owned and maintained by similar organizations working toward a common goal. In this case, the universities would all have very similar needs and calendar requirements, and they would not be financial competitors of each other. Therefore, this would be an ideal group for working together within a community cloud. A public cloud model would not work in this scenario because it is designed to serve the largest number of customers, would not likely be targeted toward specific requirements for individual customers, and would not be willing to make changes for them. A private cloud could accommodate such needs, but would not meet the criteria for a group working together, and a hybrid cloud spanning multiple cloud providers would not fit the specifics of the question.

QUESTION 24
Data centers have enormous power resources that are distributed and consumed throughout the entire facility.

Which of the following standards pertains to the proper fire safety standards within that scope?

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

Answer: C
Explanation:
The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers. The International Data Center Authority (IDCA) offers the Infinity Paradigm, which takes a macro-level approach to data center design.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**