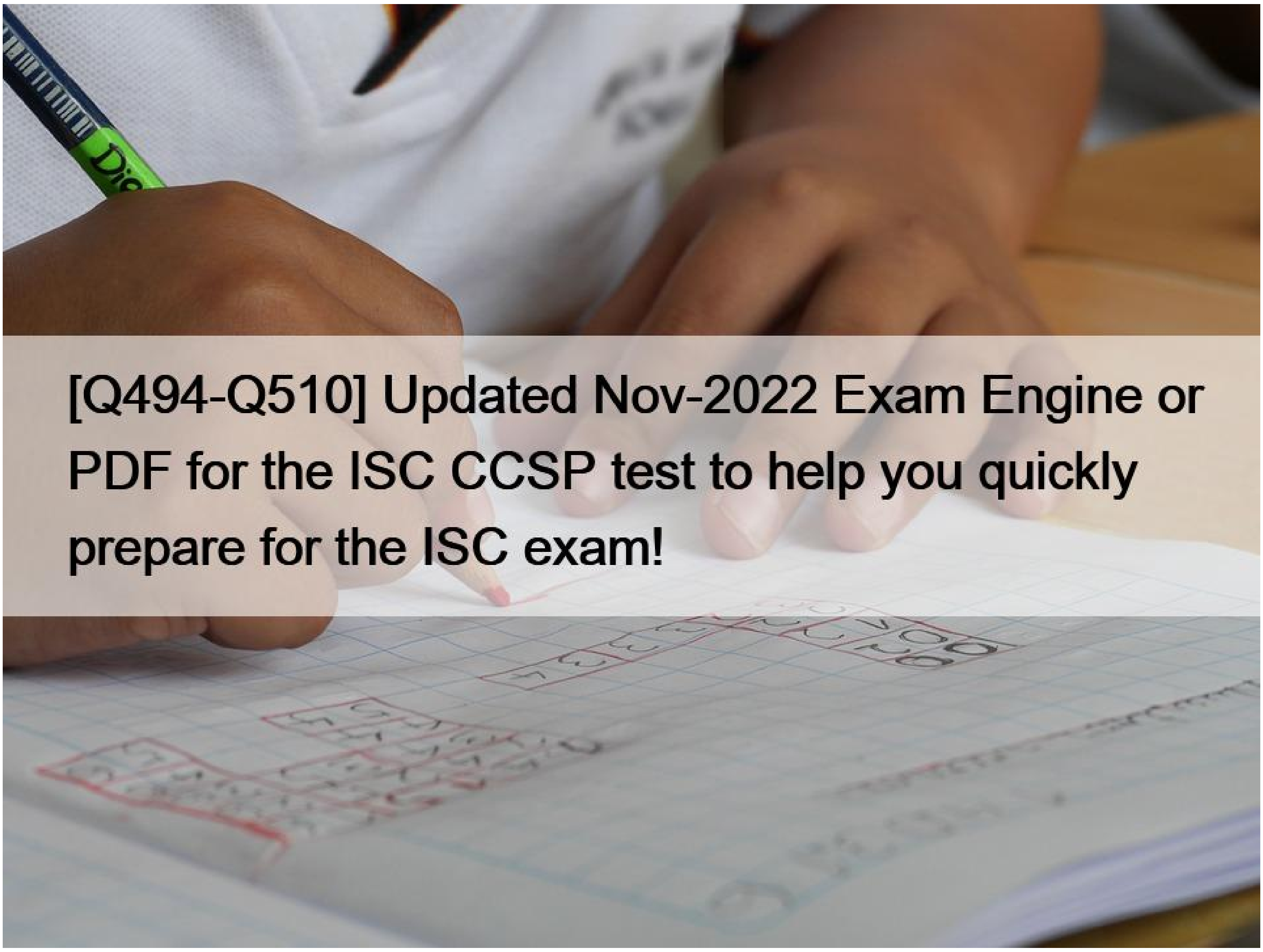
[Q494-Q510 Updated Nov-2022 Exam Engine or PDF for the ISC CCSP test to help you quickly prepare for the ISC exam!



Updated Nov-2022 Test Engine or PDF for the ISC CCSP test to help you quickly prepare for the ISC exam! Full CCSP Practice Test and 830 unique questions with explanations waiting just for you, get it now! QUESTION 494

Which of the following publishes the most commonly used standard for data center design in regard to tiers and topologies?
* IDCA
* Uptime Institute
* NFPA
* BICSI
The Uptime Institute publishes the most commonly used and widely known standard on data center tiers and topologies. It is based on a series of four tiers, with each progressive increase in number representing more stringent, reliable, and redundant systems for security, connectivity, fault tolerance, redundancy, and cooling.

QUESTION 495

An audit against the ___________ will demonstrate that an organization has a holistic, comprehensive security program.

Response:
* SAS 70 standard
* SSAE 16 standard
* SOC 2, Type 2 report matrix
* ISO 27001 certification requirements

QUESTION 496

The management plane is used to administer a cloud environment and perform administrative tasks across a variety of systems, but most specifically it&#8217;s used with the hypervisors.

What does the management plane typically leverage for this orchestration?
* APIs
* Scripts
* TLS
* XML
The management plane uses APIs to execute remote calls across the cloud environment to various management systems, especially hypervisors. This allows a centralized administrative interface, often a web portal, to orchestrate tasks throughout an enterprise. Scripts may be utilized to execute API calls, but they are not used directly to interact with systems. XML is used for data encoding and transmission, but not for executing remote calls. TLS is used to encrypt communications and may be used with API calls, but it is not the actual process for executing commands.

QUESTION 497

Your IT steering committee has, at a high level, approved your project to begin using cloud services. However, the committee is concerned with getting locked into a single cloud provider and has flagged the ability to easily move between cloud providers as a top priority. It also wants to save costs by reusing components.

Which cross-cutting aspect of cloud computing would be your primary focus as your project plan continues to develop and you begin to evaluate cloud providers?
* Interoperability
* Resiliency
* Scalability
* Portability
Interoperability is ability to easily move between cloud providers, by either moving or reusing components and services. This can pertain to any cloud deployment model, and it gives organizations the ability to constantly evaluate costs and services as well as move their business to another cloud provider as needed or desired.

Portability relates to the wholesale moving of services from one cloud provider to another, not necessarily the reuse of components or services for other purposes. Although resiliency is not an official concept within cloud computing, it certainly would be found throughout other topics such as elasticity, auto-scaling, and resource pooling. Scalability pertains to changing resource allocations to a service to meet current demand, either upward or downward in scope.

QUESTION 498

What can tokenization be used for?

Response:

* Encryption
* Compliance with PCI DSS
* Enhancing the user experience
* Giving management oversight to e-commerce functions

QUESTION 499

Which type of controls are the SOC Type 1 reports specifically focused on?
* Integrity
* PII
* Financial
* Privacy
Explanation/Reference:

Explanation:

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

QUESTION 500

Which of the following is NOT a major regulatory framework?
* PCI DSS
* HIPAA
* SOX
* FIPS 140-2
FIPS 140-2 is a United States certification standard for cryptographic modules, and it provides guidance and requirements for their use based on the requirements of the data classification. However, these are not actual regulatory requirements. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS) are all major regulatory frameworks either by law or specific to an industry.

QUESTION 501

Which of the following threat types involves an application that does not validate authorization for portions of itself after the initial checks?
* Injection
* Missing function-level access control
* Cross-site request forgery
* Cross-site scripting
Explanation

It is imperative that an application perform checks when each function or portion of the application is accessed, to ensure that the user is properly authorized to access it. Without continual checks each time a function is accessed, an attacker could forge requests to access portions of the application where authorization has not been granted.

QUESTION 502

When an organization is considering the use of cloud services for BCDR planning and solutions, which of the following cloud concepts would be the most important?
* Reversibility
* Elasticity

* Interoperability
* Portability

Portability is the ability for a service or system to easily move among different cloud providers. This is essential for using a cloud solution for BCDR because vendor lock-in would inhibit easily moving and setting up services in the event of a disaster, or it would necessitate a large number of configuration or component changes to implement. Interoperability, or the ability to reuse components for other services or systems, would not be an important factor for BCDR. Reversibility, or the ability to remove all data quickly and completely from a cloud environment, would be important at the end of a disaster, but would not be important during setup and deployment. Elasticity, or the ability to resize resources to meet current demand, would be very beneficial to a BCDR situation, but not as vital as portability.

QUESTION 503

The various models generally available for cloud BC/DR activities include all of the following except:

* Private architecture, cloud backup
* Cloud provider, backup from another cloud provider
* Cloud provider, backup from same provider
* Cloud provider, backup from private provider

This is not a normal configuration and would not likely provide genuine benefit.

QUESTION 504

Every security program and process should have which of the following?

* Severe penalties
* Multifactor authentication
* Foundational policy
* Homomorphic encryption

Policy drives all programs and functions in the organization; the organization should not conduct any operations that don&#8217;t have a policy governing them. Penalties may or may not be an element of policy, and severity depends on the topic. Multifactor authentication and homomorphic encryption are red herrings here.

QUESTION 505

What type of data does data rights management (DRM) protect?

* Consumer
* PII
* Financial
* Healthcare

DRM applies to the protection of consumer media, such as music, publications, video, movies, and soon.

QUESTION 506

Which of the following threats from the OWASP Top Ten is the most difficult for an organization to protect against?

Response:

* Advanced persistent threats
* Account hijacking
* Malicious insiders
* Denial of service

QUESTION 507

When is a virtual machine susceptible to attacks while a physical server in the same state would not be?
* When it is behind a WAF
* When it is behind an IPS
* When it is not patched
* When it is powered off
A virtual machine is ultimately an image file residing a file system. Because of this, even when a virtual machine is &#8220;powered off,&#8221; it is still susceptible to attacks and modification. A physical server that is powered off would not be susceptible to attacks.

QUESTION 508

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?
* Portability
* Virtualization
* Elasticity
* Resource pooling
Explanation/Reference:

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 509

Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company&#8217;s website)?
* SOC 1
* SOC 2, Type 1
* SOC 2, Type 2
* SOC 3

QUESTION 510

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?
* Puppet
* SCCM
* Chef

* GitHub
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.