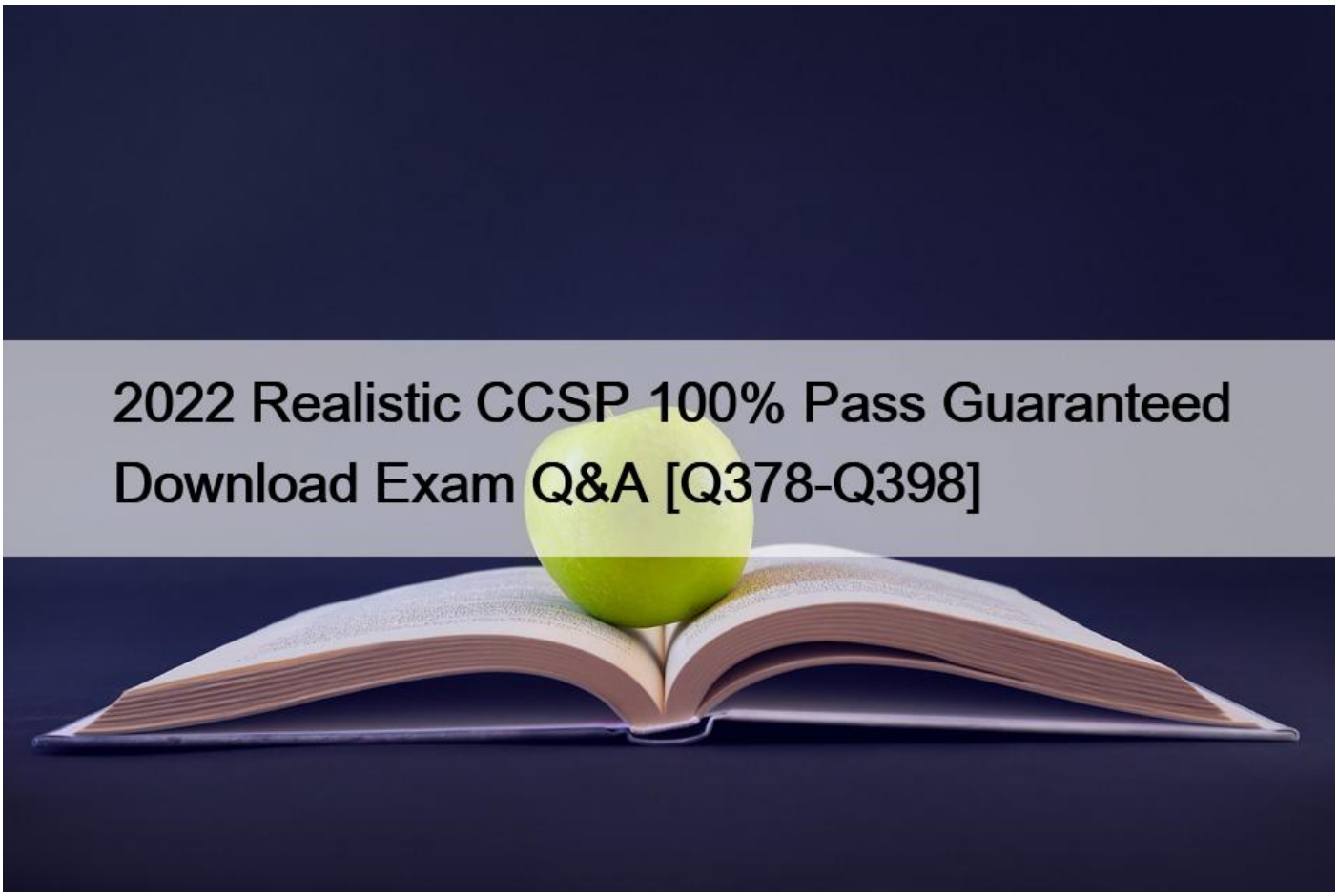
2022 Realistic CCSP 100% Pass Guaranteed Download Exam Q&A [Q378-Q398



2022 Realistic CCSP 100% Pass Guaranteed Download Exam Q&A Accurate CCSP Answers 365 Days Free Updates

Conclusion

Getting CCSP certified will not be easy, nevertheless, your right effort put in place with the right resources can help you excel at this exam. Make sure you cover all your learning objectives by referring yourself to the comprehensive study guides from Amazon and the test success is guaranteed.

NO.378 What are the U.S. State Department controls on technology exports known as?
* DRM
* ITAR
* EAR
* EAL

Explanation

ITAR is a Department of State program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Digital rights management tools are used for protecting electronic processing of intellectual property.

NO.379 Which of the following security technologies is commonly used to give administrators access into trust zones within an environment?
* VPN
* WAF
* IPSec
* HTTPS

Virtual private networks (VPNs) are commonly used to allow access into trust zones. Via a VPN, access can be controlled and logged and only allowed through secure channels by authorized users. It also adds an additional layer of encryption and protection to communications.

NO.380 Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company’s website)?
* SOC 1
* SOC 2, Type 1
* SOC 2, Type 2
* SOC 3

NO.381 A loosely coupled storage cluster will have performance and capacity limitations based on the _____.

Response:
* Physical backplane connecting it
* Total number of nodes in the cluster
* Amount of usage demanded
* The performance and capacity in each node

NO.382 Although encryption can help an organization to effectively decrease the possibility of data breaches, which other type of threat can it increase the chances of?
* Insecure interfaces
* Data loss
* System vulnerabilities
* Account hijacking

NO.383 There are many situations when testing a BCDR plan is appropriate or mandated.

Which of the following would not be a necessary time to test a BCDR plan?
* After software updates
* After regulatory changes
* After major configuration changes
* Annually

Regulatory changes by themselves would not trigger a need for new testing of a BCDR plan. Any changes necessary for regulatory compliance would be accomplished through configuration changes or software updates, which in turn would then trigger the necessary new testing. Annual testing is crucial to any BCDR plan. Also, any time major configuration changes or software updates are done, the plan should be evaluated and tested to ensure it is still valid and complete.

NO.384 Which phase of the cloud data lifecycle would be the MOST appropriate for the use of DLP technologies to protect the data?
* Use
* Store
* Share
* Create

Explanation

During the share phase, data is allowed to leave the application for consumption by other vendors, systems, or services. At this point, as the data is leaving the security controls of the application, the use of DLP technologies is appropriate to control how the data is used or to force expiration. During the use, create, and store phases, traditional security controls are available and are more appropriate because the data is still internal to the application.

NO.385 Different types of audits are intended for different audiences, such as internal, external, regulatory, and so on.

Which of the following audits are considered “restricted use” versus being for a more broad audience?
* SOC Type 2
* SOC Type 1
* SOC Type 3
* SAS-70

Explanation

SOC Type 1 reports are intended for restricted use, only to be seen by the actual service organization, its current clients, or its auditors. These reports are not intended for wider or public distribution.SAS-70 audit reports have been deprecated and are no longer in use, and both the SOC Type 2 and 3 reports are designed to expand upon the SOC Type 1 reports and are for broader audiences.

NO.386 Hardening the operating system refers to all of the following except:
* Limiting administrator access
* Closing unused ports
* Removing antimalware agents
* Removing unnecessary services and libraries

Removing antimalware agents. Hardening the operating system means making it more secure.

Limiting administrator access, closing unused ports, and removing unnecessary services and libraries all have the potential to make an OS more secure. But removing antimalware agents would actually make the system less secure. If anything, antimalware agents should be added, not removed.

NO.387 Which of the following represents a prioritization of applications or cloud customers for the allocation of additional requested resources when there is a limitation on available resources?
* Provision
* Limit
* Reservation
* Share

The concept of shares within a cloud environment is used to mitigate and control the request for resource allocations from customers that the environment may not have the current capability to allow. Shares work by prioritizing hosts within a cloud environment through a weighting system that is defined by the cloud provider. When periods of high utilization and allocation are reached, the system automatically uses scoring of each host based on its share value to determine which hosts get access to the limited resources still available. The higher the value a particular host has, the more resources it will be allowed to utilize.

NO.388 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/Reference:

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.

NO.389 The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “unvalidated redirects and forwards.” Which of the following is a good way to protect against this problem?
* Don’t use redirects/forwards in your applications.
* Refrain from storing credentials long term.
* Implement security incident/event monitoring (security information and event management (SIEM)/security information management (SIM)/security event management (SEM)) solutions.
* Implement digital rights management (DRM) solutions.

NO.390 Which entity requires all collection and storing of data on their citizens to be done on hardware that resides within their borders?
* Russia
* France
* Germany
* United States
Explanation

Explanation:

Signed into law and effective starting on September 1, 2015, Russian Law 526-FZ establishes that any collecting, storing, or processing of personal information or data on Russian citizens must be done from systems and databases that are physically located with the Russian Federation.

NO.391 Hardening the operating system refers to all of the following except:
* Limiting administrator access
* Closing unused ports
* Removing antimalware agents
* Removing unnecessary services and libraries
Explanation/Reference:

Explanation:

Removing antimalware agents. Hardening the operating system means making it more secure. Limiting administrator access, closing unused ports, and removing unnecessary services and libraries all have the potential to make an OS more secure. But removing antimalware agents would actually make the system less secure. If anything, antimalware agents should be added, not removed.

NO.392 Which of the following is NOT a focus or consideration of an internal audit?
* Certification
* Design
* Costs
* Operational efficiency
In order to obtain and comply with certifications, independent external audits must be performed and satisfied.

Although some testing of certification controls can be part of an internal audit, they will not satisfy requirements.

NO.393 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.

NO.394 Which of the following is NOT one of five principles of SOC Type 2 audits?
* Privacy
* Processing integrity
* Financial
* Security

Explanation

The SOC Type 2 audits include five principles: security, privacy, processing integrity, availability, and confidentiality.

NO.395 The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet). In a typical TLS session, who initiates the protocol?
* The server
* The client
* The certifying authority
* The ISP

NO.396 What concept does the A represent within the DREAD model?
* Affected users
* Authorization
* Authentication
* Affinity

The concept of affected users measures the percentage of users who would be impacted by a successful exploit. Scoring ranges from 0, which would impact no users, to 10, which would impact all users. None of the other options provided is the correct term.

NO.397 Resolving resource contentions in the cloud will most likely be the job of the

_____.

Response:
* Router
* Emulator
* Regulator
* Hypervisor

NO.398 What is the concept of isolating an application from the underlying operating system for testing purposes?
* Abstracting
* Application virtualization
* Hosting
* Sandboxing

Application virtualization is a software implementation that allows applications and programs to run in an isolated environment rather than directly interacting with the operating system.

Sandboxing refers to segregating information or processes for security or testing purposes, but it’s not directly related to isolation from the underlying operating system. Abstracting sounds similar to the correct term but is not pertinent to the question, and hosting is provided as an erroneous answer.