

Exam Questions CCSP

Certified Cloud Security Professional

<https://www.2passeasy.com/dumps/CCSP/>



NEW QUESTION 1

- (Exam Topic 1)

What is the term that describes the situation when a malicious user/attacker can exit the restrictions of a single host and access other nodes on the network?

Response:

- A. Host escape
- B. Guest escape
- C. Provider exit
- D. Escalation of privileges

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

DLP can be combined with what other security technology to enhance data controls? Response:

- A. DRM
- B. SIEM
- C. Kerberos
- D. Hypervisors

Answer: A

NEW QUESTION 3

- (Exam Topic 1)

According to the (ISC)2 Cloud Secure Data Life Cycle, which phase comes soon after (or at the same time as) the Create phase?

- A. Store
- B. Use
- C. Deploy
- D. Archive

Answer: A

NEW QUESTION 4

- (Exam Topic 1)

Which strategy involves using a fake production system to lure attackers in order to learn about their tactics?

Response:

- A. IDS
- B. Honeypot
- C. IPS
- D. Firewall

Answer: B

NEW QUESTION 5

- (Exam Topic 1)

Which cloud storage type uses an opaque value or descriptor to categorize and organize data? Response:

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

Answer: D

NEW QUESTION 6

- (Exam Topic 1)

The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing.

According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing?

Response:

- A. Cloud customers and third parties are continually enhancing and modifying APIs.
- B. APIs can have automated settings.
- C. It is impossible to uninstall APIs.
- D. APIs are a form of malware.

Answer: A

NEW QUESTION 7

- (Exam Topic 1)

What type of device is often leveraged to assist legacy applications that may not have the programmatic capability to process assertions from modern web services?

- A. Web application firewall
- B. XML accelerator
- C. Relying party
- D. XML firewall

Answer: B

NEW QUESTION 8

- (Exam Topic 1)

The cloud deployment model that features organizational ownership of the hardware and infrastructure, and usage only by members of that organization, is known as:

Response:

- A. Private
- B. Public
- C. Hybrid
- D. Motive

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

What is used with a single sign-on system for authentication after the identity provider has successfully authenticated a user?

Response:

- A. Token
- B. Key
- C. XML
- D. SAML

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

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? Response:

- A. Don't use redirects/forwards in your applications.
- B. Refrain from storing credentials long term.
- C. Implement security incident/event monitoring (security information and event management (SIEM)/security information management (SIM)/security event management (SEM)) solutions.
- D. Implement digital rights management (DRM) solutions.

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

Which of the following should occur at each stage of the SDLC?

- A. Added functionality
- B. Management review
- C. Verification and validation
- D. Repurposing of any newly developed components

Answer: C

NEW QUESTION 14

- (Exam Topic 1)

Which concept of cloud computing pertains to the ability to reuse components and services of an application for other purposes?

- A. Portability
- B. Interoperability
- C. Resource pooling
- D. Elasticity

Answer: B

NEW QUESTION 17

- (Exam Topic 1)

Which of the following is a file server that provides data access to multiple, heterogeneous machines/users on the network?

Response:

- A. Storage area network (SAN)
- B. Network-attached storage (NAS)
- C. Hardware security module (HSM)

D. Content delivery network (CDN)

Answer: B

NEW QUESTION 18

- (Exam Topic 1)

Which of the following best describes data masking? Response:

- A. A method where the last few numbers in a dataset are not obscure
- B. These are often used for authentication.
- C. A method for creating similar but inauthentic datasets used for software testing and user training.
- D. A method used to protect prying eyes from data such as social security numbers and credit card data.
- E. Data masking involves stripping out all similar digits in a string of numbers so as to obscure the original number.

Answer: B

NEW QUESTION 19

- (Exam Topic 1)

Which of the following is not a factor an organization might use in the cost-benefit analysis when deciding whether to migrate to a cloud environment? Response:

- A. Pooled resources in the cloud
- B. Shifting from capital expenditures to support IT investment to operational expenditures
- C. The time savings and efficiencies offered by the cloud service
- D. Branding associated with which cloud provider might be selected

Answer: D

NEW QUESTION 23

- (Exam Topic 1)

You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment. In order to get truly holistic coverage of your environment, you should be sure to include _____ as a step in the deployment process. Response:

- A. Getting signed user agreements from all users
- B. Installation of the solution on all assets in the cloud data center
- C. Adoption of the tool in all routers between your users and the cloud provider
- D. All of your customers to install the tool

Answer: A

NEW QUESTION 27

- (Exam Topic 1)

You work for a government research facility. Your organization often shares data with other government research organizations. You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations. Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources. If you don't use cross-certification, what other model can you implement for this purpose? Response:

- A. Third-party identity broker
- B. Cloud reseller
- C. Intractable nuanced variance
- D. Mandatory access control (MAC)

Answer: A

NEW QUESTION 32

- (Exam Topic 1)

At which phase of the SDLC process should security begin participating?

- A. Requirements gathering
- B. Requirements analysis
- C. Design
- D. Testing

Answer: A

NEW QUESTION 34

- (Exam Topic 1)

Because PaaS implementations are so often used for software development, what is one of the vulnerabilities that should always be kept in mind? Response:

- A. Malware
- B. Loss/theft of portable devices
- C. Backdoors
- D. DoS/DDoS

Answer: C

NEW QUESTION 37

- (Exam Topic 1)

You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment. What should you not expect the tool to address? Response:

- A. Sensitive data sent inadvertently in user emails
- B. Sensitive data captured by screen shots
- C. Sensitive data moved to external devices
- D. Sensitive data in the contents of files sent via FTP

Answer: B

NEW QUESTION 40

- (Exam Topic 1)

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 “cross-site scripting (XSS).” Which of the following is not a method for reducing the risk of XSS attacks? Response:

- A. Use an auto-escaping template system.
- B. XML escape all identity assertions.
- C. Sanitize HTML markup with a library designed for the purpose.
- D. HTML escape JSON values in an HTML context and read the data with JSON.parse.

Answer: B

NEW QUESTION 41

- (Exam Topic 1)

Which of the following is considered an administrative control?

- A. Access control process
- B. Keystroke logging
- C. Door locks
- D. Biometric authentication

Answer: A

NEW QUESTION 43

- (Exam Topic 1)

Every cloud service provider that opts to join the CSA STAR program registry must complete a _____.

- A. SOC 2, Type 2 audit report
- B. Consensus Assessment Initiative Questionnaire (CAIQ)
- C. NIST 800-37 RMF audit
- D. ISO 27001 ISMS review

Answer: B

NEW QUESTION 45

- (Exam Topic 1)

Different types of cloud deployment models use different types of storage from traditional data centers, along with many new types of software platforms for deploying applications and configurations. Which of the following is NOT a storage type used within a cloud environment?

- A. Docker
- B. Object
- C. Structured
- D. Volume

Answer: A

NEW QUESTION 48

- (Exam Topic 1)

Which of the following types of organizations is most likely to make use of open source software technologies?

- A. Government agencies
- B. Corporations
- C. Universities
- D. Military

Answer: C

NEW QUESTION 50

- (Exam Topic 1)

Which of the following is a possible negative aspect of bit-splitting?

- A. Greater chance of physical theft of assets
- B. Loss of public image
- C. Some risk to availability, depending on the implementation
- D. A small fire hazard

Answer: C

NEW QUESTION 51

- (Exam Topic 1)

Why are PaaS environments at a higher likelihood of suffering backdoor vulnerabilities?

- A. They rely on virtualization.
- B. They are often used for software development.
- C. They have multitenancy.
- D. They are scalable.

Answer: B

NEW QUESTION 55

- (Exam Topic 1)

Which of the following data sanitation methods would be the MOST effective if you needed to securely remove data as quickly as possible in a cloud environment?

Response:

- A. Zeroing
- B. Cryptographic erasure
- C. Overwriting
- D. Degaussing

Answer: B

NEW QUESTION 60

- (Exam Topic 1)

You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider.

Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also allow users to select which APIs they install and use on their own devices in order to access and manipulate company data.

Of the following, what is a security control you'd like to implement to offset the risk(s) incurred by this practice?

- A. Regular and widespread integrity checks on sampled data throughout the managed environment
- B. More extensive and granular background checks on all employees, particularly new hires
- C. Inclusion of references to all applicable regulations in the policy documents
- D. Increased enforcement of separation of duties for all workflows

Answer: A

NEW QUESTION 61

- (Exam Topic 1)

DAST checks software functionality in _____.

Response:

- A. The production environment
- B. A runtime state
- C. The cloud
- D. An IaaS configuration

Answer: B

NEW QUESTION 65

- (Exam Topic 1)

A firewall can use all of the following techniques for controlling traffic except:

- A. Rule sets
- B. Behavior analysis
- C. Content filtering
- D. Randomization

Answer: D

NEW QUESTION 66

- (Exam Topic 1)

A honeypot can be used for all the following purposes except _____.

Response:

- A. Gathering threat intelligence
- B. Luring attackers
- C. Distracting attackers
- D. Delaying attackers

Answer: B

NEW QUESTION 71

- (Exam Topic 1)

Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:
Response:

- A. The cloud provider's suppliers
- B. The cloud provider's vendors
- C. The cloud provider's utilities
- D. The cloud provider's resellers

Answer: D

NEW QUESTION 72

- (Exam Topic 1)

The physical layout of a cloud data center campus should include redundancies of all the following except
_____.
Response:

- A. Generators
- B. HVAC units
- C. Generator fuel storage
- D. Points of personnel ingress

Answer: D

NEW QUESTION 74

- (Exam Topic 1)

Log data should be protected _____.
Response:

- A. One level below the sensitivity level of the systems from which it was collected
- B. At least at the same sensitivity level as the systems from which it was collected
- C. With encryption in transit, at rest, and in use
- D. According to NIST guidelines

Answer: B

NEW QUESTION 78

- (Exam Topic 1)

Using one cloud provider for your operational environment and another for your BCDR backup will also give you the additional benefit of _____.
Response:

- A. Allowing any custom VM builds you use to be instantly ported to another environment
- B. Avoiding vendor lock-in/lockout
- C. Increased performance
- D. Lower cost

Answer: B

NEW QUESTION 82

- (Exam Topic 1)

Which concept pertains to cloud customers paying only for the resources they use and consume, and only for the duration they are using them?
Response:

- A. Measured service
- B. Auto-scaling
- C. Portability
- D. Elasticity

Answer: A

NEW QUESTION 86

- (Exam Topic 1)

Which of the following is not typically included as a basic phase of the software development life cycle?

- A. Define
- B. Design
- C. Describe
- D. Develop

Answer: C

NEW QUESTION 90

- (Exam Topic 1)

What are the phases of a software development lifecycle process model? Response:

- A. Planning and requirements analysis, define, design, develop, testing, and maintenance
- B. Define, planning and requirements analysis, design, develop, testing, and maintenance
- C. Planning and requirements analysis, define, design, testing, develop, and maintenance
- D. Planning and requirements analysis, design, define, develop, testing, and maintenance

Answer: A

NEW QUESTION 91

- (Exam Topic 1)

Data labels could include all the following, except: Response:

- A. Source
- B. Delivery vendor
- C. Handling restrictions
- D. Jurisdiction

Answer: B

NEW QUESTION 95

- (Exam Topic 1)

DRM solutions should generally include all the following functions, except:

- A. Persistency
- B. Automatic self-destruct
- C. Automatic expiration
- D. Dynamic policy control

Answer: B

NEW QUESTION 96

- (Exam Topic 1)

You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Previous releases have shipped with major flaws that were not detected in the testing phase; leadership wants to avoid repeating that problem. What tool/technique/technology might you suggest to aid in identifying programming errors?

- A. Vulnerability scans
- B. Open source review
- C. SOC audits
- D. Regulatory review

Answer: B

NEW QUESTION 98

- (Exam Topic 1)

Which cloud service category offers the most customization options and control to the cloud customer? Response:

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

Answer: B

NEW QUESTION 101

- (Exam Topic 1)

SOX was enacted because of which of the following? Response:

- A. Poor BOD oversight
- B. Lack of independent audits
- C. Poor financial controls
- D. All of the above

Answer: D

NEW QUESTION 106

- (Exam Topic 1)

Application virtualization can typically be used for .

- A. Denying access to untrusted users
- B. Detecting and mitigating DDoS attacks
- C. Replacing encryption as a necessary control
- D. Running an application on an endpoint without installing it

Answer: D

NEW QUESTION 108

- (Exam Topic 1)

Which of the following management risks can make an organization's cloud environment unviable? Response:

- A. Insider trading
- B. VM sprawl
- C. Hostile takeover
- D. Improper personnel selection

Answer: B

NEW QUESTION 110

- (Exam Topic 1)

Which of the following best describes a cloud carrier?

- A. A person or entity responsible for making a cloud service available to consumers
- B. The intermediary who provides connectivity and transport of cloud services between cloud providers and cloud consumers
- C. The person or entity responsible for keeping cloud services running for customers
- D. The person or entity responsible for transporting data across the Internet

Answer: B

NEW QUESTION 113

- (Exam Topic 1)

Which of the following is not a reason for conducting audits?

- A. Regulatory compliance
- B. User satisfaction
- C. Determination of service quality
- D. Security assurance

Answer: B

NEW QUESTION 117

- (Exam Topic 1)

The use of which of the following technologies will NOT require the security dependency of an operating system, other than its own?

- A. Management plane
- B. Type 1 hypervisor
- C. Type 2 hypervisor
- D. Virtual machine

Answer: B

NEW QUESTION 122

- (Exam Topic 1)

_____ is the most prevalent protocol used in identity federation.

- A. HTTP
- B. SAML
- C. FTP
- D. WS-Federation

Answer: B

NEW QUESTION 124

- (Exam Topic 1)

What are the six components that make up the STRIDE threat model? Response:

- A. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
- B. Spoofing, Tampering, Non-Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
- C. Spoofing, Tampering, Repudiation, Information Disclosure, Distributed Denial of Service, and Elevation of Privilege
- D. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Social Engineering

Answer: A

NEW QUESTION 125

- (Exam Topic 1)

The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet). In a typical TLS session, what is the usual means for establishing trust between the parties?

Response:

- A. Out-of-band authentication

- B. Multifactor authentication
- C. PKI certificates
- D. Preexisting knowledge of each other

Answer: C

NEW QUESTION 128

- (Exam Topic 2)

While an audit is being conducted, which of the following could cause management and the auditors to change the original plan in order to continue with the audit? Response:

- A. Cost overruns
- B. Impact on systems
- C. Regulatory changes
- D. Software version changes

Answer: A

NEW QUESTION 130

- (Exam Topic 2)

You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment. Which of these activities should you perform before deploying the tool? Response:

- A. Survey your company's departments about the data under their control
- B. Reconstruct your firewalls
- C. Harden all your routers
- D. Adjust the hypervisors

Answer: A

NEW QUESTION 131

- (Exam Topic 2)

What is the intellectual property protection for the logo of a new video game? Response:

- A. Copyright
- B. Patent
- C. Trademark
- D. Trade secret

Answer: C

NEW QUESTION 136

- (Exam Topic 2)

Which SSAE 16 audit report is simply an attestation of audit results? Response:

- A. SOC 1
- B. SOC 2, Type 1
- C. SOC 2, Type 2
- D. SOC 3

Answer: D

NEW QUESTION 140

- (Exam Topic 2)

A process for _____ can aid in protecting against data disclosure due to lost devices. Response:

- A. User punishment
- B. Credential revocation
- C. Law enforcement notification
- D. Device tracking

Answer: B

NEW QUESTION 143

- (Exam Topic 2)

In a Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a _____. Response:

- A. Domain name (DN)
- B. Distinguished name (DN)
- C. Directory name (DN)
- D. Default name (DN)

Answer: B

NEW QUESTION 145

- (Exam Topic 2)

You are the data manager for a retail company; you anticipate a much higher volume of sales activity in the final quarter of each calendar year than the other quarters.

In order to handle these increased transactions, and to accommodate the temporary sales personnel you will hire for only that time period, you consider augmenting your internal, on-premises production environment with a cloud capability for a specific duration, and will return to operating fully on-premises after the period of increased activity.

This is an example of _____.

Response:

- A. Cloud framing
- B. Cloud enhancement
- C. Cloud fragility
- D. Cloud bursting

Answer: D

NEW QUESTION 146

- (Exam Topic 2)

A bare-metal hypervisor is Type _____.

Response:

- A. 1
- B. 2
- C. 3
- D. 4

Answer: A

NEW QUESTION 148

- (Exam Topic 2)

Which key storage solution would be the BEST choice in a situation where availability might be of a particular concern?

Response:

- A. Internal
- B. External
- C. Hosted
- D. Embedded

Answer: A

NEW QUESTION 152

- (Exam Topic 2)

Which cloud service category is MOST likely to use a client-side key management system? Response:

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

Answer: B

NEW QUESTION 155

- (Exam Topic 2)

The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) addresses all the following security architecture elements except _____.

Response:

- A. Physical security
- B. IaaS
- C. Application security
- D. Business drivers

Answer: D

NEW QUESTION 156

- (Exam Topic 2)

The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program has _____ tiers.

Response:

- A. Two
- B. Three
- C. Four
- D. Eight

Answer: B

NEW QUESTION 161

- (Exam Topic 2)

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?
Response:

- A. Insecure interfaces
- B. Data loss
- C. System vulnerabilities
- D. Account hijacking

Answer: B

NEW QUESTION 162

- (Exam Topic 2)

Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?

Response:

- A. Persistence
- B. Influence
- C. Resistance
- D. Trepidation

Answer: A

NEW QUESTION 166

- (Exam Topic 2)

In a cloud environment, encryption should be used for all the following, except: Response:

- A. Long-term storage of data
- B. Near-term storage of virtualized images
- C. Secure sessions/VPN
- D. Profile formatting

Answer: D

NEW QUESTION 170

- (Exam Topic 2)

Which of the following is not one of the types of controls? Response:

- A. Transitional
- B. Administrative
- C. Technical
- D. Physical

Answer: A

NEW QUESTION 173

- (Exam Topic 2)

The physical layout of a cloud data center campus should include redundancies of all the following except _____.

Response:

- A. Physical perimeter security controls (fences, lights, walls, etc.)
- B. The administration/support staff building
- C. Electrical utility lines
- D. Communications connectivity lines

Answer: B

NEW QUESTION 178

- (Exam Topic 2)

Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?

Response:

- A. Unvalidated redirects and forwards
- B. Cross-site request forgery
- C. Cross-site scripting
- D. Insecure direct object references

Answer: A

NEW QUESTION 182

- (Exam Topic 2)

Who should be involved in review and maintenance of user accounts/access? Response:

- A. The user's manager
- B. The security manager
- C. The accounting department

D. The incident response team

Answer: A

NEW QUESTION 184

- (Exam Topic 2)

Which of the following is NOT one of the cloud computing activities, as outlined in ISO/IEC 17789? Response:

- A. Cloud service provider
- B. Cloud service partner
- C. Cloud service administrator
- D. Cloud service customer

Answer: C

NEW QUESTION 186

- (Exam Topic 2)

Which of the following is a method for apportioning resources that involves setting maximum usage amounts for all tenants/customers within the environment? Response:

- A. Reservations
- B. Shares
- C. Cancellations
- D. Limits

Answer: D

NEW QUESTION 189

- (Exam Topic 2)

A cloud data encryption situation where the cloud customer retains control of the encryption keys and the cloud provider only processes and stores the data could be considered a _____. Response:

- A. Threat
- B. Risk
- C. Hybrid cloud deployment model
- D. Case of infringing on the rights of the provider

Answer: C

NEW QUESTION 190

- (Exam Topic 2)

What is the risk to the organization posed by dashboards that display data discovery results? Response:

- A. Increased chance of external penetration
- B. Flawed management decisions based on massaged displays
- C. Higher likelihood of inadvertent disclosure
- D. Raised incidence of physical theft

Answer: B

NEW QUESTION 194

- (Exam Topic 2)

Administrative penalties for violating the General Data Protection Regulation (GDPR) can range up to _____. Response:

- A. US\$100,000
- B. 500,000 euros
- C. 20,000,000 euros
- D. 1,000,000 euros

Answer: C

NEW QUESTION 195

- (Exam Topic 2)

Although performing BCDR tests at regular intervals is a best practice to ensure processes and documentation are still relevant and efficient, which of the following represents a reason to conduct a BCDR review outside of the regular interval? Response:

- A. Staff changes
- B. Application changes
- C. Regulatory changes
- D. Management changes

Answer: B

NEW QUESTION 200

- (Exam Topic 2)

Firewalls can detect attack traffic by using all these methods except _____.

Response:

- A. Known past behavior in the environment
- B. Identity of the malicious user
- C. Point of origination
- D. Signature matching

Answer: B

NEW QUESTION 202

- (Exam Topic 2) What does nonrepudiation mean?

Response:

- A. Prohibiting certain parties from a private conversation
- B. Ensuring that a transaction is completed before saving the results
- C. Ensuring that someone cannot turn off auditing capabilities while performing a function
- D. Preventing any party that participates in a transaction from claiming that it did not

Answer: D

NEW QUESTION 207

- (Exam Topic 2)

Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider? Response:

- A. SOC 1 Type 1
- B. SOC 2 Type 2
- C. SOC 1 Type 2
- D. SOC 3

Answer: D

NEW QUESTION 209

- (Exam Topic 2)

Which type of software is most likely to be reviewed by the most personnel, with the most varied perspectives?

Response:

- A. Database management software
- B. Open source software
- C. Secure software
- D. Proprietary software

Answer: B

NEW QUESTION 212

- (Exam Topic 2)

There are two general types of smoke detectors. Which type uses a small portion of radioactive material? Response:

- A. Photoelectric
- B. Ionization
- C. Electron pulse
- D. Integral field

Answer: B

NEW QUESTION 214

- (Exam Topic 2)

All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline, except _____.

Response:

- A. Audit the baseline to ensure that all configuration items have been included and applied correctly
- B. Impose the baseline throughout the environment
- C. Capture an image of the baseline system for future reference/versioning/rollback purposes
- D. Document all baseline configuration elements and versioning data

Answer: B

NEW QUESTION 216

- (Exam Topic 2)

Which of the following contract terms most incentivizes the cloud provider to meet the requirements listed in the SLA?

Response:

- A. Regulatory oversight
- B. Financial penalties
- C. Performance details

D. Desire to maintain customer satisfaction

Answer: B

NEW QUESTION 220

- (Exam Topic 2)

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 “using components with known vulnerabilities.”

Why would an organization ever use components with known vulnerabilities to create software? Response:

- A. The organization is insured.
- B. The particular vulnerabilities only exist in a context not being used by developers.
- C. Some vulnerabilities only exist in foreign countries.
- D. A component might have a hidden vulnerability.

Answer: B

NEW QUESTION 221

- (Exam Topic 2)

Halon is now illegal to use for data center fire suppression. What is the reason it was outlawed? Response:

- A. It poses a threat to health and human safety when deployed.
- B. It can harm the environment.
- C. It does not adequately suppress fires.
- D. It causes undue damage to electronic systems.

Answer: B

NEW QUESTION 223

- (Exam Topic 2)

What principle must always been included with an SOC 2 report? Response:

- A. Confidentiality
- B. Security
- C. Privacy
- D. Processing integrity

Answer: B

NEW QUESTION 227

- (Exam Topic 2)

Each of the following is an element of the Identification phase of the identity and access management (IAM) process except _____.

Response:

- A. Provisioning
- B. Inversion
- C. Management
- D. Deprovisioning

Answer: B

NEW QUESTION 231

- (Exam Topic 2)

What aspect of data center planning occurs first? Response:

- A. Logical design
- B. Physical design
- C. Audit
- D. Policy revision

Answer: B

NEW QUESTION 232

- (Exam Topic 2)

Which phase of the cloud data lifecycle also typically entails the process of data classification? Response:

- A. Use
- B. Store
- C. Create
- D. Archive

Answer: C

NEW QUESTION 237

- (Exam Topic 2)

Which of the following is a risk associated with manual patching especially in the cloud?

Response:

- A. No notice before the impact is realized
- B. Lack of applicability to the environment
- C. Patches may or may not address the vulnerability they were designed to fix.
- D. The possibility for human error

Answer: D

NEW QUESTION 238

- (Exam Topic 2)

Which of the following is a possible negative aspect of bit-splitting? Response:

- A. It may require trust in additional third parties beyond the primary cloud service provider.
- B. There may be cause for management concern that the technology will violate internal policy.
- C. Users will have far greater difficulty understanding the implementation.
- D. Limited vendors make acquisition and support challenging.

Answer: A

NEW QUESTION 243

- (Exam Topic 2)

The Restatement (Second) Conflict of Law refers to which of the following? Response:

- A. The basis for deciding which laws are most appropriate in a situation where conflicting laws exist
- B. When judges restate the law in an opinion
- C. How jurisdictional disputes are settled
- D. Whether local or federal laws apply in a situation

Answer: A

NEW QUESTION 247

- (Exam Topic 2)

Which of the following in a federated environment is responsible for consuming authentication tokens? Response:

- A. Relying party
- B. Identity provider
- C. Cloud services broker
- D. Authentication provider

Answer: A

NEW QUESTION 251

- (Exam Topic 2)

Which type of report is considered for “general” use and does not contain any sensitive information? Response:

- A. SOC 1
- B. SAS-70
- C. SOC 3
- D. SOC 2

Answer: C

NEW QUESTION 254

- (Exam Topic 2)

Of the following, which is probably the most significant risk in a managed cloud environment? Response:

- A. DDoS
- B. Management plane breach
- C. Guest escape
- D. Physical attack on the utility service lines

Answer: B

NEW QUESTION 256

- (Exam Topic 2)

DLP solutions typically involve all of the following aspects except _____.

Response:

- A. Data discovery
- B. Tokenization
- C. Monitoring
- D. Enforcement

Answer: B

NEW QUESTION 258

- (Exam Topic 2)

_____ can often be the result of inadvertent activity. Response:

- A. DDoS
- B. Phishing
- C. Sprawl
- D. Disasters

Answer: C

NEW QUESTION 261

- (Exam Topic 2)

When considering the option to migrate from an on-premises environment to a hosted cloud service, an organization should weigh the risks of allowing external entities to access the cloud data for collaborative purposes against _____.

Response:

- A. Not securing the data in the legacy environment
- B. Disclosing the data publicly
- C. Inviting external personnel into the legacy workspace in order to enhance collaboration
- D. Sending the data outside the legacy environment for collaborative purposes

Answer: D

NEW QUESTION 264

- (Exam Topic 2)

What is the primary security mechanism used to protect SOAP and REST APIs? Response:

- A. Firewalls
- B. XML firewalls
- C. Encryption
- D. WAFs

Answer: C

NEW QUESTION 266

- (Exam Topic 2)

You are the IT director for a small contracting firm. Your company is considering migrating to a cloud production environment.

Which service model would best fit your needs if you wanted an option that reduced the chance of vendor lock-in but also did not require the highest degree of administration by your own personnel?

Response:

- A. IaaS
- B. PaaS
- C. SaaS
- D. TanstaafL

Answer: B

NEW QUESTION 268

- (Exam Topic 2)

Which of the following data protection methodologies maintains the ability to connect back values to the original values?

Response:

- A. Tokenization
- B. Anonymization
- C. Obfuscation
- D. Dynamic mapping

Answer: A

NEW QUESTION 272

- (Exam Topic 2)

From a security perspective, automation of configuration aids in _____.

Response:

- A. Enhancing performance
- B. Reducing potential attack vectors
- C. Increasing ease of use of the systems
- D. Reducing need for administrative personnel

Answer: B

NEW QUESTION 273

- (Exam Topic 3)

Which of the following is NOT one of the security domains presented within the Cloud Controls Matrix? Response:

- A. Financial security
- B. Mobile security
- C. Data center security
- D. Interface security

Answer: A

NEW QUESTION 278

- (Exam Topic 3)

Why might an organization choose to comply with the ISO 27001 standard?

Response:

- A. Price
- B. Ease of implementation
- C. International acceptance
- D. Speed

Answer: C

NEW QUESTION 281

- (Exam Topic 3)

Federation allows _____ across organizations.

Response:

- A. Role replication
- B. Encryption
- C. Policy
- D. Access

Answer: D

NEW QUESTION 282

- (Exam Topic 3)

Which technology is most associated with tunneling? Response:

- A. IPSec
- B. GRE
- C. IaaS
- D. XML

Answer: B

NEW QUESTION 284

- (Exam Topic 3)

The nature of cloud computing and how it operates make complying with data discovery and disclosure orders more difficult. Which of the following concepts provides the biggest challenge in regard to data collection, pursuant to a legal order?

Response:

- A. Portability
- B. Multitenancy
- C. Reversibility
- D. Auto-scaling

Answer: B

NEW QUESTION 289

- (Exam Topic 3)

Which network protocol is essential for allowing automation and orchestration within a cloud environment? Response:

- A. DNSSEC
- B. DHCP
- C. IPsec
- D. VLANs

Answer: B

NEW QUESTION 292

- (Exam Topic 3)

Which of the following aspects of the BC/DR process poses a risk to the organization? Response:

- A. Threat intelligence gathering
- B. Preplacement of response assets
- C. Budgeting for disaster
- D. Full testing of the plan

Answer: D

NEW QUESTION 294

- (Exam Topic 3)

Devices in the cloud datacenter should be secure against attack. All the following are means of hardening devices, except:

Response:

- A. Using a strong password policy
- B. Removing default passwords
- C. Strictly limiting physical access
- D. Removing all admin accounts

Answer: D

NEW QUESTION 299

- (Exam Topic 3)

Typically, SSDs are _____.

Response:

- A. More expensive than spinning platters
- B. Larger than tape backup
- C. Heavier than tape libraries
- D. More subject to malware than legacy drives

Answer: A

NEW QUESTION 303

- (Exam Topic 3)

A cloud provider is looking to provide a higher level of assurance to current and potential cloud customers about the design and effectiveness of their security controls.

Which of the following audit reports would the cloud provider choose as the most appropriate to accomplish this goal?

Response:

- A. SAS-70
- B. SOC 1
- C. SOC 2
- D. SOC 3

Answer: D

NEW QUESTION 307

- (Exam Topic 3)

Fiber-optic lines are considered part of layer _____ of the OSI model. Response:

- A. 1
- B. 3
- C. 5
- D. 7

Answer: A

NEW QUESTION 310

- (Exam Topic 3)

Digital rights management (DRM) tools can be combined with _____, to enhance security capabilities. Response:

- A. Roaming identity services (RIS)
- B. Egress monitoring solutions (DLP)
- C. Internal hardware settings (BIOS)
- D. Remote Authentication Dial-In User Service (RADIUS)

Answer: B

NEW QUESTION 311

- (Exam Topic 3)

Which of the following is not a component of the STRIDE model? Response:

- A. Spoofing
- B. Repudiation
- C. Information disclosure
- D. External pen testing

Answer: D

NEW QUESTION 314

- (Exam Topic 3)

Cloud environments are based entirely on virtual machines and virtual devices, and those images are also in need of storage within the environment. What type of storage is typically used for virtual images?

Response:

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

Answer: D

NEW QUESTION 317

- (Exam Topic 3)

Which of the following is an example of useful and sufficient data masking of the string “CCSP”? Response:

- A. XCSP
- B. PSCC
- C. TtLp
- D. 3X91

Answer: C

NEW QUESTION 318

- (Exam Topic 3)

The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. A cloud customer that does not perform sufficient due diligence can suffer harm if the cloud provider they've selected goes out of business.

What do we call this problem? Response:

- A. Vendor lock-in
- B. Vendor lock-out
- C. Vendor incapacity
- D. Unscaled

Answer: B

NEW QUESTION 323

- (Exam Topic 3)

What type of redundancy can we expect to find in a datacenter of any tier?

Response:

- A. All operational components
- B. All infrastructure
- C. Emergency egress
- D. Full power capabilities

Answer: C

NEW QUESTION 326

- (Exam Topic 3)

DLP solutions can aid all of the following security-related efforts except _____.

Response:

- A. Access control
- B. Egress monitoring
- C. e-discovery/forensics
- D. Data categorization/classification

Answer: A

NEW QUESTION 327

- (Exam Topic 3)

What is the cloud service model in which the customer is responsible for administration of the OS? Response:

- A. IaaS
- B. PaaS
- C. SaaS
- D. QaaS

Answer: A

NEW QUESTION 332

- (Exam Topic 3)

FM-200 has all the following properties except _____.

Response:

- A. It's nontoxic at levels used for fire suppression
- B. It's gaseous at room temperature
- C. It may deplete the Earth's ozone layer
- D. It does not leave a film or coagulant after use

Answer: C

NEW QUESTION 336

- (Exam Topic 3)

Your company maintains an on-premises data center for daily production activities but wants to use a cloud service to augment this capability during times of increased demand (cloud bursting).

Which deployment model would probably best suit the company's needs? Response:

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

Answer: D

NEW QUESTION 337

- (Exam Topic 3)

You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally.

Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes. Your company has decided to expand its business to include selling and monitoring life-support equipment for medical providers.

What characteristic do you need to ensure is offered by your cloud provider? Response:

- A. Full automation of security controls within the cloud data center
- B. Tier 4 of the Uptime Institute certifications
- C. Global remote access
- D. Prevention of ransomware infections

Answer: B

NEW QUESTION 339

- (Exam Topic 3)

What is the major difference between authentication/authorization? Response:

- A. Code verification/code implementation
- B. Identity validation/access permission
- C. Inverse incantation/obverse instantiation
- D. User access/privileged access

Answer: B

NEW QUESTION 341

- (Exam Topic 3)

Which theoretical technology would allow superposition of physical states to increase both computing capacity and encryption keyspace? Response:

- A. All-or-nothing-transform with Reed-Solomon (AONT-RS)
- B. Quantum computing
- C. Filigree investment
- D. Sharding

Answer: B

NEW QUESTION 345

- (Exam Topic 3)

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 "injection."

In most cases, what is the method for reducing the risk of an injection attack? Response:

- A. User training
- B. Hardening the OS
- C. Input validation/bounds checking
- D. Physical locks

Answer: C

NEW QUESTION 348

- (Exam Topic 3)

What aspect of a Type 2 hypervisor involves additional security concerns that are not relevant with a Type 1 hypervisor? Response:

- A. Reliance on a host operating system
- B. Auditing
- C. Proprietary software
- D. Programming languages

Answer: A

NEW QUESTION 350

- (Exam Topic 3)

Virtual machine (VM) configuration management (CM) tools should probably include _____.

Response:

- A. Biometric recognition
- B. Anti-tampering mechanisms
- C. Log file generation
- D. Hackback capabilities

Answer: C

NEW QUESTION 355

- (Exam Topic 3)

Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like: Response:

- A. Syn floods
- B. Ransomware
- C. XSS and SQL injection
- D. Password cracking

Answer: C

NEW QUESTION 357

- (Exam Topic 3)

Which characteristic of automated patching makes it attractive? Response:

- A. Cost
- B. Speed
- C. Noise reduction
- D. Capability to recognize problems quickly

Answer: B

NEW QUESTION 362

- (Exam Topic 3)

Which ISO/IEC standards set documents the cloud definitions for staffing and official roles? Response:

- A. ISO/IEC 27001
- B. ISO/IEC 17788
- C. ISO/IEC 17789
- D. ISO/IEC 27040

Answer: B

NEW QUESTION 365

- (Exam Topic 3)

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

Response:

- A. SAS 70 standard
- B. SSAE 16 standard
- C. SOC 2, Type 2 report matrix
- D. ISO 27001 certification requirements

Answer: D

NEW QUESTION 370

- (Exam Topic 3)

Which of the following is a risk that stems from a virtualized environment? Response:

- A. Live virtual machines in the production environment are moved from one host to another in the clear.
- B. Cloud data centers can become a single point of failure.
- C. It is difficult to find and contract with multiple utility providers of the same type (electric, water, etc.).
- D. Modern SLA demands are stringent and very hard to meet.

Answer: A

NEW QUESTION 371

- (Exam Topic 3) Who operates the management plane? Response:

- A. Regulators
- B. End consumers
- C. Privileged users
- D. Privacy data subjects

Answer:

C

NEW QUESTION 374

- (Exam Topic 3)

Your company has just been served with an eDiscovery order to collect event data and other pertinent information from your application during a specific period of time, to be used as potential evidence for a court proceeding.

Which of the following, apart from ensuring that you collect all pertinent data, would be the MOST important consideration?

Response:

- A. Encryption
- B. Chain of custody
- C. Compression
- D. Confidentiality

Answer: B

NEW QUESTION 377

- (Exam Topic 3)

In which of the following situations does the data owner have to administer the OS? Response:

- A. IaaS
- B. PaaS
- C. Offsite archive
- D. SaaS

Answer: A

NEW QUESTION 379

- (Exam Topic 3)

What is the term used to describe loss of access to data because the cloud provider has ceased operation? Response:

- A. Closing
- B. Vendor lock-out
- C. Vendor lock-in
- D. Masking

Answer: B

NEW QUESTION 380

- (Exam Topic 3)

In general, a cloud BCDR solution will be _____ than a physical solution. Response:

- A. Slower
- B. Less expensive
- C. Larger
- D. More difficult to engineer

Answer: B

NEW QUESTION 385

- (Exam Topic 3)

It is important to include _____ in the design of underfloor plenums if they are also used for wiring. Response:

- A. Mantraps
- B. Sequestered channels
- C. Heat sinks
- D. Tight gaskets

Answer: D

NEW QUESTION 388

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CCSP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CCSP Product From:

<https://www.2passeasy.com/dumps/CCSP/>

Money Back Guarantee

CCSP Practice Exam Features:

- * CCSP Questions and Answers Updated Frequently
- * CCSP Practice Questions Verified by Expert Senior Certified Staff
- * CCSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CCSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year