

Exam Questions CCSP

Certified Cloud Security Professional

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



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 2

- (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 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 of the following is characterized by a set maximum capacity? Response:

- A. A secret-sharing-made-short (SSMS) bit-splitting implementation
- B. A tightly coupled cloud storage cluster
- C. A loosely coupled cloud storage cluster
- D. A public-key infrastructure

Answer: B

NEW QUESTION 5

- (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 6

- (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 7

- (Exam Topic 1)

What is the federal agency that accepts applications for new patents?

- A. USDA
- B. USPTO
- C. OSHA
- D. SEC

Answer: B

NEW QUESTION 8

- (Exam Topic 1)

Which of the following best describes SAML? Response:

- A. A standard for developing secure application management logistics
- B. A standard for exchanging authentication and authorization data between security domains
- C. A standard for exchanging usernames and passwords across devices
- D. A standard used for directory synchronization

Answer: B

NEW QUESTION 9

- (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 10

- (Exam Topic 1)

Which phase of the cloud data lifecycle involves processing by a user or application? Response:

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

Answer: D

NEW QUESTION 10

- (Exam Topic 1)

Which of the following are contractual components that the CSP should review and understand fully when contracting with a cloud service provider? (Choose two.)

- A. Concurrently maintainable site infrastructure
- B. Use of subcontractors
- C. Redundant site infrastructure capacity components
- D. Scope of processing

Answer: BD

NEW QUESTION 14

- (Exam Topic 1)

A typical DLP tool can enhance the organization's efforts at accomplishing what legal task? Response:

- A. Evidence collection
- B. Delivering testimony
- C. Criminal prosecution
- D. Enforcement of intellectual property rights

Answer: A

NEW QUESTION 15

- (Exam Topic 1)

You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization. Which of the following benefits will the CSA CCM offer your organization? Response:

- A. Simplifying regulatory compliance
- B. Collecting multiple data streams from your log files
- C. Ensuring that the baseline configuration is applied to all systems
- D. Enforcing contract terms between your organization and the cloud provider

Answer: A

NEW QUESTION 20

- (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 21

- (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 25

- (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 30

- (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 35

- (Exam Topic 1)

Which of the following is a method for apportioning resources that involves setting guaranteed minimums for all tenants/customers within the environment?

Response:

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

Answer: A

NEW QUESTION 38

- (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)

Who is ultimately responsible for a data breach that includes personally identifiable information (PII), in the event of negligence on the part of the cloud provider?

- A. The user
- B. The subject

- C. The cloud provider
- D. The cloud customer

Answer: D

NEW QUESTION 44

- (Exam Topic 1)

Which of the following is not one of the defined security controls domains within the Cloud Controls Matrix, published by the Cloud Security Alliance?

Response:

- A. Financial
- B. Human resources
- C. Mobile security
- D. Identity and access management

Answer: A

NEW QUESTION 49

- (Exam Topic 1)

What sort of legal enforcement may the Payment Card Industry (PCI) Security Standards Council not bring to bear against organizations that fail to comply with the Payment Card Industry Data Security Standard (PCI DSS)?

Response:

- A. Fines
- B. Jail time
- C. Suspension of credit card processing privileges
- D. Subject to increased audit frequency and scope

Answer: B

NEW QUESTION 50

- (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 54

- (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 57

- (Exam Topic 1)

Which of the following practices can enhance both operational capabilities and configuration management efforts?

Response:

- A. Regular backups
- B. Constant uptime
- C. Multifactor authentication
- D. File hashes

Answer: D

NEW QUESTION 59

- (Exam Topic 1)

TLS uses _____ to authenticate a connection and create a shared secret for the duration of the session.

- A. SAML 2.0
- B. X.509 certificates
- C. 802.11X
- D. The Diffie-Hellman process

Answer: B

NEW QUESTION 62

- (Exam Topic 1)

In the cloud motif, the data processor is usually: Response:

- A. The party that assigns access rights
- B. The cloud customer
- C. The cloud provider
- D. The cloud access security broker

Answer: C

NEW QUESTION 65

- (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 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 68

- (Exam Topic 1)

One of the security challenges of operating in the cloud is that additional controls must be placed on file storage systems because _____.

Response:

- A. File stores are always kept in plain text in the cloud
- B. There is no way to sanitize file storage space in the cloud
- C. Virtualization necessarily prevents the use of application-based security controls
- D. Virtual machines are stored as snapshotted files when not in use

Answer: D

NEW QUESTION 70

- (Exam Topic 1)

All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:

Response:

- A. Tokenization
- B. Data discovery
- C. Obfuscation
- D. Masking

Answer: B

NEW QUESTION 73

- (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 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 80

- (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 84

- (Exam Topic 1)

Which ISO standard refers to addressing security risks in a supply chain?

- A. ISO 27001
- B. ISO/IEC 28000:2007
- C. ISO 18799
- D. ISO 31000:2009

Answer: B

NEW QUESTION 85

- (Exam Topic 1)

What is the amount of fuel that should be on hand to power generators for backup datacenter power, in all tiers, according to the Uptime Institute?

- A. 1
- B. 1,000 gallons
- C. 12 hours
- D. As much as needed to ensure all systems may be gracefully shut down and data securely stored

Answer: C

NEW QUESTION 88

- (Exam Topic 1)

Who is the entity identified by personal data? Response:

- A. The data owner
- B. The data processor
- C. The data custodian
- D. The data subject

Answer: D

NEW QUESTION 89

- (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 91

- (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 95

- (Exam Topic 1)

A honeypot should contain data_____.

Response:

- A. Raw
- B. Production
- C. Useless
- D. Sensitive

Answer: C

NEW QUESTION 99

- (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 increase the security value of the DLP, you should consider combining it with _____.

Response:

- A. Digital rights management (DRM) and security event and incident management (SIEM) tools
- B. An investment in upgraded project management software
- C. Digital insurance policies
- D. The Uptime Institute's Tier certification

Answer: A

NEW QUESTION 104

- (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, all of the following activity can result in data loss except _____ .

- A. Misplaced crypto keys
- B. Improper policy
- C. Ineffectual backup procedures
- D. Accidental overwrite

Answer: B

NEW QUESTION 109

- (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 112

- (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 115

- (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 119

- (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 124

- (Exam Topic 2)

What could be the result of failure of the cloud provider to secure the hypervisor in such a way that one user on a virtual machine can see the resource calls of another user's virtual machine?

Response:

- A. Unauthorized data disclosure
- B. Inference attacks
- C. Social engineering
- D. Physical intrusion

Answer: B

NEW QUESTION 126

- (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 130

- (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 132

- (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 134

- (Exam Topic 2)

Which of the following BCDR testing methodologies is least intrusive? Response:

- A. Walk-through
- B. Simulation
- C. Tabletop
- D. Full test

Answer: C

NEW QUESTION 138

- (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 143

- (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 147

- (Exam Topic 2)

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 aspect of managed cloud services makes the threat of malicious insiders so alarming?

Response:

- A. Scalability
- B. Multitenancy
- C. Metered service
- D. Flexibility

Answer: B

NEW QUESTION 152

- (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 154

- (Exam Topic 2)

The destruction of a cloud customer's data can be required by all of the following except _____.

Response:

- A. Statute
- B. Regulation
- C. The cloud provider's policy
- D. Contract

Answer: C

NEW QUESTION 155

- (Exam Topic 2)

Which of the following are not examples of personnel controls? Response:

- A. Background checks
- B. Reference checks
- C. Strict access control mechanisms
- D. Continuous security training

Answer: C

NEW QUESTION 157

- (Exam Topic 2)

Which of the following is NOT a core component of an SIEM solution? Response:

- A. Correlation
- B. Aggregation
- C. Compliance
- D. Escalation

Answer: D

NEW QUESTION 160

- (Exam Topic 2)

You are the IT security manager for a video game software development company. Which of the following is most likely to be your primary concern on a daily basis?

Response:

- A. Health and human safety
- B. Security flaws in your products
- C. Security flaws in your organization
- D. Regulatory compliance

Answer: C

NEW QUESTION 164

- (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 169

- (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 171

- (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 176

- (Exam Topic 2)

Which of the following would NOT be included as input into the requirements gathering for an application or system?

Response:

- A. Users
- B. Management
- C. Regulators
- D. Auditors

Answer: D

NEW QUESTION 177

- (Exam Topic 2)

Before deploying a specific brand of virtualization toolset, it is important to configure it according to _____.

Response:

- A. Industry standards
- B. Prevailing law of that jurisdiction
- C. Vendor guidance
- D. Expert opinion

Answer: C

NEW QUESTION 181

- (Exam Topic 2)

Why does the physical location of your data backup and/or BCDR failover environment matter? Response:

- A. It may affect regulatory compliance
- B. Lack of physical security
- C. Environmental factors such as humidity
- D. It doesn't matter
- E. Data can be saved anywhere without consequence

Answer: A

NEW QUESTION 183

- (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 185

- (Exam Topic 2)

Which of the following is the correct name for Tier II of the Uptime Institute Data Center Site Infrastructure Tier Standard Topology?

Response:

- A. Concurrently Maintainable Site Infrastructure
- B. Fault-Tolerant Site Infrastructure
- C. Basic Site Infrastructure
- D. Redundant Site Infrastructure Capacity Components

Answer: D

NEW QUESTION 186

- (Exam Topic 2)

Single sign-on systems work by authenticating users from a centralized location or using a centralized method, and then allowing applications that trust the system to grant those users access. What would be passed between the authentication system and the applications to grant a user access?

Response:

- A. Ticket
- B. Certificate
- C. Credential
- D. Token

Answer: D

NEW QUESTION 188

- (Exam Topic 2)

Your organization is considering a move to a cloud environment and is looking for certifications or audit reports from cloud providers to ensure adequate security controls and processes.

Which of the following is NOT a security certification or audit report that would be pertinent? Response:

- A. FedRAMP
- B. PCI DSS
- C. FIPS 140-2
- D. SOC Type 2

Answer: C

NEW QUESTION 191

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 193

- (Exam Topic 2)

All of the following are identity federation standards commonly found in use today except _____.

Response:

- A. WS-Federation
- B. OpenID
- C. OAuth

D. PGP

Answer: D

NEW QUESTION 196

- (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 197

- (Exam Topic 2) What are SOCI/SOCII/SOCIII? Response:

- A. Risk management frameworks
- B. Access controls
- C. Audit reports
- D. Software development phases

Answer: C

NEW QUESTION 202

- (Exam Topic 2) What is a key component of GLBA? Response:

- A. The right to be forgotten
- B. EU Data Directives
- C. The information security program
- D. The right to audit

Answer: C

NEW QUESTION 204

- (Exam Topic 2)

When designing a cloud data center, which of the following aspects is not necessary to ensure continuity of operations during contingency operations? Response:

- A. Access to clean water
- B. Broadband data connection
- C. Extended battery backup
- D. Physical access to the data center

Answer: C

NEW QUESTION 208

- (Exam Topic 2)

Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company's website)?

Response:

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

Answer: D

NEW QUESTION 210

- (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 214

- (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 216

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 217

- (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 221

- (Exam Topic 2)

Aside from the fact that the cloud customer probably cannot locate/reach the physical storage assets of the cloud provider, and that wiping an entire storage space would impact other customers, why would degaussing probably not be an effective means of secure sanitization in the cloud? Response:

- A. All the data storage space in the cloud is already gaussed.
- B. Cloud data storage may not be affected by degaussing.
- C. Federal law prohibits it in the United States.
- D. The blast radius is too wide.

Answer: B

NEW QUESTION 226

- (Exam Topic 2)

Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality? Response:

- A. Obfuscation
- B. Masking
- C. Tokenization
- D. Anonymization

Answer: C

NEW QUESTION 229

- (Exam Topic 2)

Which of the following is not a way to manage risk? Response:

- A. Enveloping
- B. Mitigating
- C. Accepting
- D. Transferring

Answer: A

NEW QUESTION 232

- (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 235

- (Exam Topic 3)
Federation allows _____ across organizations.
Response:

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

Answer: D

NEW QUESTION 236

- (Exam Topic 3)
The BCDR plan/process should be written and documented in such a way that it can be used by _____.
Response:

- A. Users
- B. Essential BCDR team members
- C. Regulators
- D. Someone with the requisite skills

Answer: D

NEW QUESTION 239

- (Exam Topic 3)
Which technology is most associated with tunneling? Response:

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

Answer: B

NEW QUESTION 243

- (Exam Topic 3)
Which kind of SSAE report comes with a seal of approval from a certified auditor? Response:

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

Answer: C

NEW QUESTION 247

- (Exam Topic 3)
Which of the following methods for the safe disposal of electronic records can always be used in a cloud environment? Response:

- A. Physical destruction
- B. Encryption
- C. Overwriting
- D. Degaussing

Answer: B

NEW QUESTION 251

- (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 253

- (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 257

- (Exam Topic 3)

The Brewer-Nash security model is also known as which of the following? Response:

- A. MAC
- B. The Chinese Wall model
- C. Preventive measures
- D. RBAC

Answer: B

NEW QUESTION 260

- (Exam Topic 3)

Access should be based on _____.

Response:

- A. Regulatory mandates
- B. Business needs and acceptable risk
- C. User requirements and management requests
- D. Optimum performance and security provision

Answer: B

NEW QUESTION 262

- (Exam Topic 3)

If bit-splitting is used to store data sets across multiple jurisdictions, how may this enhance security? Response:

- A. By making seizure of data by law enforcement more difficult
- B. By hiding it from attackers in a specific jurisdiction
- C. By ensuring that users can only accidentally disclose data to one geographic area
- D. By restricting privilege user access

Answer: A

NEW QUESTION 267

- (Exam Topic 3)

What is the main reason virtualization is used in the cloud? Response:

- A. VMs are easier to administer
- B. If a VM is infected with malware, it can be easily replaced
- C. With VMs, the cloud provider does not have to deploy an entire hardware device for every new user
- D. VMs are easier to operate than actual devices

Answer: C

NEW QUESTION 268

- (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 269

- (Exam Topic 3)

The ISO/IEC 27001:2013 security standard contains 14 different domains that cover virtually all areas of IT operations and procedures. Which of the following is NOT one of the domains listed in the standard?

Response:

- A. Legal
- B. Management
- C. Assets
- D. Supplier Relationships

Answer: A

NEW QUESTION 272

- (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 “security misconfiguration.” Which of these is a technique to reduce the potential for a security misconfiguration? Response:

- A. Get regulatory approval for major configuration modifications.
- B. Update the BCDR plan on a timely basis.
- C. Train all users on proper security procedures.
- D. Perform periodic scans and audits of the environment.

Answer: D

NEW QUESTION 277

- (Exam Topic 3)

Cryptographic keys for encrypted data stored in the cloud should be _____.

Response:

- A. At least 128 bits long
- B. Not stored with the cloud provider
- C. Split into groups
- D. Generated with redundancy

Answer: B

NEW QUESTION 279

- (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 280

- (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 282

- (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 286

- (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 289

- (Exam Topic 3)

What type of identity system allows trust and verifications between the authentication systems of multiple organizations?

Response:

- A. Federated
- B. Collaborative
- C. Integrated
- D. Bidirectional

Answer: A

NEW QUESTION 293

- (Exam Topic 3)

Which type of web application monitoring most closely measures actual activity? Response:

- A. Synthetic performance monitoring
- B. Real-user monitoring (RUM)
- C. Security information and event management (SIEM)
- D. Database application monitor (DAM)

Answer: B

NEW QUESTION 297

- (Exam Topic 3)

It's important to maintain a current asset inventory list, including surveying your environment on a regular basis, in order to _____.
Response:

- A. Prevent unknown, unpatched assets from being used as back doors to the environment
- B. Ensure that any lost devices are automatically entered into the acquisition system for repurchasing and replacement
- C. Maintain user morale by having their devices properly catalogued and annotated
- D. Ensure that billing for all devices is handled by the appropriate departments

Answer: A

NEW QUESTION 300

- (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 302

- (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 307

- (Exam Topic 3)

What are the objectives of change management? (Choose all that apply.)

Response:

- A. Respond to a customer's changing business requirements while maximizing value and reducing incidents, disruption, and rework
- B. Ensure that changes are recorded and evaluated
- C. Respond to business and IT requests for change that will disassociate services with business needs
- D. Ensure that all changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner

Answer: AB

NEW QUESTION 308

- (Exam Topic 3)

A web application firewall (WAF) can understand and act on _____ traffic.
Response:

- A. Malicious
- B. SMTP
- C. ICMP
- D. HTTP

Answer: D

NEW QUESTION 310

- (Exam Topic 3)

In addition to BCDR, what other benefit can your data archive/backup provide? Response:

- A. Physical security enforcement
- B. Access control methodology
- C. Security control against data breach
- D. Identity management testing

Answer: D

NEW QUESTION 314

- (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 319

- (Exam Topic 3)

Security best practices in a virtualized network environment would include which of the following? Response:

- A. Using distinct ports and port groups for various VLANs on a virtual switch rather than running them through the same port
- B. Running iSCSI traffic unencrypted in order to have it observed and monitored by NIDS
- C. Adding HIDS to all virtual guests
- D. Hardening all outward-facing firewalls in order to make them resistant to attack

Answer: A

NEW QUESTION 321

- (Exam Topic 3)

Software-defined networking (SDN) is intended to separate different network capabilities and allow for the granting of granular configurations, permissions, and features to non-network staff or customers. Which network capability is separated from forwarding of traffic?

Response:

- A. Routing
- B. Firewalling
- C. Filtering
- D. IPS

Answer: C

NEW QUESTION 326

- (Exam Topic 3)

Which of the following is perhaps the best method for reducing the risk of a specific application not delivering the proper level of functionality and performance when it is moved from the legacy environment into the cloud?

Response:

- A. Remove the application from the organization's production environment, and replace it with something else.
- B. Negotiate and conduct a trial run in the cloud environment for that application before permanently migrating.
- C. Make sure the application is fully updated and patched according to all vendor specifications.
- D. Run the application in an emulator.

Answer: B

NEW QUESTION 327

.....

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