

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)

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)

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 4

- (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 5

- (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 6

- (Exam Topic 1)

Which of the following is essential for getting full security value from your system baseline? Response:

- A. Capturing and storing an image of the baseline
- B. Keeping a copy of upcoming suggested modifications to the baseline
- C. Having the baseline vetted by an objective third party
- D. Using a baseline from another industry member so as not to engage in repetitious efforts

Answer: A

NEW QUESTION 7

- (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 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 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 10

- (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 13

- (Exam Topic 1)

Cloud environments pose many unique challenges for a data custodian to properly adhere to policies and the use of data. What poses the biggest challenge for a data custodian with a PaaS implementation, over and above the same concerns with IaaS?

Response:

- A. Access to systems
- B. Knowledge of systems
- C. Data classification rules
- D. Contractual requirements

Answer: B

NEW QUESTION 18

- (Exam Topic 1)

Which of the following storage types are used with an Infrastructure as a Service (IaaS) solution? Response:

- A. Volume and block
- B. Structured and object
- C. Unstructured and ephemeral
- D. Volume and object

Answer: D

NEW QUESTION 21

- (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 23

- (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 27

- (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. Management is interested in adopting an Agile development style.

This will be typified by which of the following traits? Response:

- A. Reliance on a concrete plan formulated during the Define phase
- B. Rigorous, repeated security testing
- C. Isolated programming experts for specific functional elements
- D. Short, iterative work periods

Answer: D

NEW QUESTION 29

- (Exam Topic 1)

Which security certification serves as a general framework that can be applied to any type of system or application?

- A. ISO/IEC 27001
- B. PCI DSS
- C. FIPS 140-2
- D. NIST SP 800-53

Answer: A

NEW QUESTION 34

- (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 36

- (Exam Topic 1)

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 38

- (Exam Topic 1)

Which of the following are considered to be the building blocks of cloud computing? Response:

- A. Data, access control, virtualization, and services

- B. Storage, networking, printing and virtualization
- C. CPU, RAM, storage and networking
- D. Data, CPU, RAM, and access control

Answer: C

NEW QUESTION 40

- (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. Most of the cloud customer's interaction with resources will be performed through APIs.
- B. APIs are inherently insecure.
- C. Attackers have already published vulnerabilities for all known APIs.
- D. APIs are known carcinogens.

Answer: A

NEW QUESTION 44

- (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 49

- (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 52

- (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 54

- (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 55

- (Exam Topic 1)

When an organization considers cloud migrations, the organization's software developers will need to know which _____ and _____ which the organization will be using, in order to properly and securely create suitable applications.

- A. Geographic location, native language
- B. Legal restrictions, specific ISP
- C. Service model, deployment model
- D. Available bandwidth, telecommunications country code

Answer: C

NEW QUESTION 60

- (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 64

- (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 67

- (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 69

- (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 74

- (Exam Topic 1)

A honeypot should contain data_____.

Response:

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

Answer: C

NEW QUESTION 79

- (Exam Topic 1)

Who should be the only entity allowed to declare that an organization can return to normal following contingency or BCDR operations? Response:

- A. Regulators
- B. Law enforcement
- C. The incident manager
- D. Senior management

Answer: D

NEW QUESTION 80

- (Exam Topic 1)

Who will determine data classifications for the cloud customer?

- A. The cloud provider
- B. NIST

- C. Regulators
- D. The cloud customer

Answer: D

NEW QUESTION 81

- (Exam Topic 1)

Impact resulting from risk being realized is often measured in terms of _____.

- A. Amount of data lost
- B. Money
- C. Amount of property lost
- D. Number of people affected

Answer: B

NEW QUESTION 85

- (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 86

- (Exam Topic 1)

Which standards body depends heavily on contributions and input from its open membership base? Response:

- A. NIST
- B. ISO
- C. ICANN
- D. CSA

Answer: D

NEW QUESTION 87

- (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 89

- (Exam Topic 1)

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

- A. Confidentiality level
- B. Distribution limitations
- C. Access restrictions
- D. Multifactor authentication

Answer: D

NEW QUESTION 91

- (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 96

- (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 98

- (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 99

- (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 100

- (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 102

- (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 107

- (Exam Topic 2)

A federated identity system is composed of three main components. Which of the following is NOT one of the three main components?

Response:

- A. Identity provider
- B. User
- C. Relying party
- D. API

Answer: D

NEW QUESTION 111

- (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 115

- (Exam Topic 2)

A bare-metal hypervisor is Type _____.

Response:

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

Answer: A

NEW QUESTION 119

- (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 123

- (Exam Topic 2)

Your organization has made it a top priority that any cloud environment being considered to host production systems have guarantees that resources will always be available for allocation when needed.

Which of the following concepts will you need to ensure is part of the contract and SLA? Response:

- A. Limits
- B. Shares
- C. Resource pooling
- D. Reservations

Answer: D

NEW QUESTION 126

- (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 129

- (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 134

- (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 136

- (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 137

- (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 142

- (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 147

- (Exam Topic 2)

All of the following entities are required to use FedRAMP-accredited Cloud Service Providers except _____.

Response:

- A. The US post office
- B. The Department of Homeland Security
- C. Federal Express
- D. The CIA

Answer: C

NEW QUESTION 152

- (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 155

- (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 160

- (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 164

- (Exam Topic 2)

You are a consultant performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost \$24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant.

The fire suppression system costs \$15 million. An insurance policy that would cover the full replacement cost of the plant costs \$1 million per month.

In order to establish the true annualized loss expectancy (ALE), you would need all of the following information except _____.

Response:

- A. The amount of revenue generated by the plant
- B. The rate at which the plant generates revenue
- C. The length of time it would take to rebuild the plant
- D. The amount of product the plant creates

Answer: D

NEW QUESTION 168

- (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 171

- (Exam Topic 2)

Resolving resource contentions in the cloud will most likely be the job of the _____.

Response:

- A. Router
- B. Emulator
- C. Regulator
- D. Hypervisor

Answer: D

NEW QUESTION 172

- (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. Remove all nonessential programs from the baseline image
- B. Exclude the target system you intend to baseline from any scheduled updates/patching used in production systems
- C. Include the baseline image in the asset inventory/configuration management database
- D. Configure the host OS according to the baseline requirements

Answer: C

NEW QUESTION 175

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 180

- (Exam Topic 2)

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 182

- (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 183

- (Exam Topic 2)

Which of the following is not a feature of SAST? Response:

- A. Source code review
- B. Team-building efforts
- C. “White-box” testing
- D. Highly skilled, often expensive outside consultants

Answer: B

NEW QUESTION 185

- (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 186

- (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 187

- (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 189

- (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 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 197

- (Exam Topic 2)

Which security certification serves as a general framework that can be applied to any type of system or application?

Response:

- A. ISO/IEC 27001
- B. PCI DSS
- C. FIPS 140-2
- D. NIST SP 800-53

Answer: A

NEW QUESTION 201

- (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 206

- (Exam Topic 2)

What type of software is often considered secured and validated via community knowledge?

Response:

- A. Proprietary
- B. Object-oriented
- C. Open source
- D. Scripting

Answer: C

NEW QUESTION 207

- (Exam Topic 2)

TLS provides _____ and _____ for communications. Response:

- A. Privacy, security
- B. Security, optimization
- C. Privacy, integrity
- D. Enhancement, privacy

Answer: C

NEW QUESTION 208

- (Exam Topic 2)

You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center.

One of the challenges you're facing is whether the provider will have undue control over your data once it is within the provider's data center; will the provider be able to hold your organization hostage because they have your data?

This is a(n) _____ issue. Response:

- A. Interoperability
- B. Portability
- C. Availability
- D. Security

Answer: B

NEW QUESTION 210

- (Exam Topic 2)

All of the following might be used as data discovery characteristics in a content-analysis-based data discovery effort except _____.

Response:

- A. Keywords
- B. Pattern-matching
- C. Frequency
- D. Inheritance

Answer: D

NEW QUESTION 213

- (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 217

- (Exam Topic 2)

What is a data custodian responsible for? Response:

- A. The safe custody, transport, storage of the data, and implementation of business rules
- B. Data content, context, and associated business rules
- C. Logging and alerts for all data
- D. Customer access and alerts for all data

Answer: A

NEW QUESTION 219

- (Exam Topic 2)

You have been tasked by management to offload processing and validation of incoming encoded data from your application servers and their associated APIs.

Which of the following would be the most appropriate device or software to consider?

Response:

- A. XML accelerator
- B. XML firewall
- C. Web application firewall
- D. Firewall

Answer: A

NEW QUESTION 220

- (Exam Topic 2)

A denial of service (DoS) attack can potentially impact all customers within a cloud environment with the continued allocation of additional resources. Which of the following can be useful for a customer to protect themselves from a DoS attack against another customer?

Response:

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

Answer: B

NEW QUESTION 224

- (Exam Topic 2)

What is a cloud storage architecture that manages the data in caches of copied content close to locations of high demand?

Response:

- A. Object-based storage
- B. File-based storage
- C. Database
- D. CDN

Answer: D

NEW QUESTION 225

- (Exam Topic 2)

An audit against the _____ will demonstrate that an organization has inadequate security controls to meet its ISO 27001 requirements.

Response:

- A. SAS 70 standard

- B. SSAE 16 standard
- C. ISO 27002 certification criteria
- D. NIST SP 800-53

Answer: C

NEW QUESTION 227

- (Exam Topic 2)

Which of the following is NOT a common component of a DLP implementation process? Response:

- A. Discovery
- B. Monitoring
- C. Revision
- D. Enforcement

Answer: C

NEW QUESTION 231

- (Exam Topic 2)

Which of these characteristics of a virtualized network adds risks to the cloud environment? Response:

- A. Redundancy
- B. Scalability
- C. Pay-per-use
- D. Self-service

Answer: A

NEW QUESTION 235

- (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 236

- (Exam Topic 3)

You work for a company that operates a production environment in the cloud. Another company using the same cloud provider is under investigation by law enforcement for racketeering.

Your company should be concerned about this because of the cloud characteristic of . Response:

- A. Virtualization
- B. Pooled resources
- C. Elasticity
- D. Automated self-service

Answer: B

NEW QUESTION 237

- (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 240

- (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 241

- (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 243

- (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 246

- (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 249

- (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 250

- (Exam Topic 3)

Although indirect identifiers cannot alone point to an individual, the more of them known can lead to a specific identity. Which strategy can be used to avoid such a connection being made?

Response:

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

Answer: B

NEW QUESTION 255

- (Exam Topic 3)

When a customer performs a penetration test in the cloud, why isn't the test an optimum simulation of attack conditions?

Response:

- A. Attackers don't use remote access for cloud activity
- B. Advanced notice removes the element of surprise
- C. When cloud customers use malware, it's not the same as when attackers use malware
- D. Regulator involvement changes the attack surface

Answer: B

NEW QUESTION 260

- (Exam Topic 3)

Patches do all the following except _____.
Response:

- A. Address newly discovered vulnerabilities
- B. Solve cloud interoperability problems

- C. Add new features and capabilities to existing systems
- D. Address performance issues

Answer: B

NEW QUESTION 262

- (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 265

- (Exam Topic 3)

Which of the following data-sanitation approaches are always available within a cloud environment? Response:

- A. Physical destruction
- B. Shredding
- C. Overwriting
- D. Cryptographic erasure

Answer: D

NEW QUESTION 270

- (Exam Topic 3)

Proper _____ need to be assigned to each data classification/category. Response:

- A. Dollar values
- B. Metadata
- C. Security controls
- D. Policies

Answer: C

NEW QUESTION 275

- (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 280

- (Exam Topic 3)

A truly airgapped machine selector will _____.

Response:

- A. Terminate a connection before creating a new connection
- B. Be made of composites and not metal
- C. Have total Faraday properties
- D. Not be portable

Answer: A

NEW QUESTION 284

- (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 288

- (Exam Topic 3)

Which of the following would NOT be used to determine the classification of data?

Response:

- A. Metadata
- B. PII
- C. Creator
- D. Future use

Answer: D

NEW QUESTION 293

- (Exam Topic 3)

DLP solutions can aid in deterring loss due to which of the following?

Response:

- A. Randomization
- B. Inadvertent disclosure
- C. Natural disaster
- D. Device failure

Answer: B

NEW QUESTION 297

- (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 299

- (Exam Topic 3)

Which of the following is not included in the OWASP Top Ten web application security threats? Response:

- A. Injection
- B. Cross-site scripting
- C. Internal theft
- D. Sensitive data exposure

Answer: C

NEW QUESTION 301

- (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)

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 305

- (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 308

- (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 311

- (Exam Topic 3)

Which of the following types of software is a Type 2 hypervisor dependent on that a Type 1 hypervisor isn't? Response:

- A. VPN
- B. Firewall
- C. Operating system
- D. IDS

Answer: C

NEW QUESTION 312

- (Exam Topic 3)

In a data retention policy, what is perhaps the most crucial element? Response:

- A. Location of the data archive
- B. Frequency of backups
- C. Security controls in long-term storage
- D. Data recovery procedures

Answer: D

NEW QUESTION 313

- (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 316

- (Exam Topic 3)

Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?

Response:

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

Answer: B

NEW QUESTION 318

- (Exam Topic 3)

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.

In order to pass the user IDs and authenticating credentials of each user among the organizations, what protocol/language/motif will you most likely utilize? Response:

- A. Representational State Transfer (REST)
- B. Security Assertion Markup Language (SAML)

- C. Simple Object Access Protocol (SOAP)
- D. Hypertext Markup Language (HTML)

Answer: B

NEW QUESTION 322

- (Exam Topic 3)

Managed cloud services exist because the service is less expensive for each customer than creating the same services for themselves in a legacy environment. Using a managed service allows the customer to realize significant cost savings through the reduction of

_____.

Response:

- A. Risk
- B. Security controls
- C. Personnel
- D. Data

Answer: C

NEW QUESTION 325

- (Exam Topic 3)

_____ is perhaps the main external factor driving IAM efforts. Response:

- A. Regulation
- B. Business need
- C. The evolving threat landscape
- D. Monetary value

Answer: A

NEW QUESTION 330

- (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 334

- (Exam Topic 3)

Your application has been a continued target for SQL injection attempts. Which of the following technologies would be best used to combat the likeliness of a successful SQL injection exploit from occurring?

Response:

- A. XML accelerator
- B. WAF
- C. Sandbox
- D. Firewall

Answer: B

NEW QUESTION 338

- (Exam Topic 3)

The BIA can be used to provide information about all the following, except: Response:

- A. Risk analysis
- B. Secure acquisition
- C. BC/DR planning
- D. Selection of security controls

Answer: B

NEW QUESTION 343

- (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 348

- (Exam Topic 3)

Setting thermostat controls by measuring the temperature will result in the _____ highest energy costs. Response:

- A. Server inlet
- B. Return air
- C. Under-floor
- D. External ambient

Answer: B

NEW QUESTION 349

.....

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