



**ISC2**

**Exam Questions CCSP**

Certified Cloud Security Professional

## About Exambible

### *Your Partner of IT Exam*

## Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

- (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 2

- (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 3

- (Exam Topic 1)

Which of the following is a risk in the cloud environment that is not existing or is as prevalent in the legacy environment?

Response:

- A. Legal liability in multiple jurisdictions
- B. Loss of productivity due to DDoS
- C. Ability of users to gain access to their physical workplace
- D. Fire

**Answer:** A

#### NEW QUESTION 4

- (Exam Topic 1)

You have been tasked with creating an audit scope statement and are making your project outline. Which of the following is NOT typically included in an audit scope statement?

- A. Statement of purpose
- B. Deliverables
- C. Classification
- D. Costs

**Answer:** D

#### NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (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 9

- (Exam Topic 1)

Egress monitoring solutions usually include a function that \_\_\_\_\_.

Response:

- A. Uses biometrics to scan users
- B. Inspects incoming packets
- C. Resides on client machines
- D. Uses stateful inspection

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 1)

Which of the following is the best and only completely secure method of data destruction? Response:

- A. Degaussing
- B. Crypto-shredding
- C. Physical destruction of resources that store the data
- D. Legal order issued by the prevailing jurisdiction where the data is geographically situated

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 1)

You are performing an audit of the security controls used in a cloud environment. Which of the following would best serve your purpose?

Response:

- A. The business impact analysis (BIA)
- B. A copy of the VM baseline configuration
- C. The latest version of the company's financial records
- D. A SOC 3 report from another (external) auditor

**Answer:** B

#### NEW QUESTION 13

- (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 16

- (Exam Topic 1)

The cloud deployment model that features joint ownership of assets among an affinity group is known as: Response:

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

**Answer:** D

#### NEW QUESTION 20

- (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 23

- (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 26

- (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 29

- (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 31

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 32

- (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 36

- (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 38

- (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 40

- (Exam Topic 1) 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 42

- (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 47

- (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 50

- (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, an organization that suffers a data breach might suffer all of the following negative effects except \_\_\_\_\_. Response:

- A. Cost of compliance with notification laws
- B. Loss of public perception/goodwill
- C. Loss of market share
- D. Cost of detection

**Answer:** D

#### NEW QUESTION 54

- (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 56

- (Exam Topic 1)

During which stage of the SDLC process should security be consulted and begin its initial involvement?

- A. Testing
- B. Design
- C. Development
- D. Requirement gathering

**Answer:** D

#### NEW QUESTION 57

- (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 61

- (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 63

- (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 68

- (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 71

- (Exam Topic 1)

A honeypot should contain data\_\_\_\_\_.

Response:

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

**Answer:** C

#### NEW QUESTION 76

- (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 77

- (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 82

- (Exam Topic 1)

At which layer does the IPSec protocol operate to encrypt and protect communications between two parties? Response:

- A. Network
- B. Application
- C. Transport
- D. Data link

**Answer:** A

#### NEW QUESTION 83

- (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 88

- (Exam Topic 1)

When using transparent encryption of a database, where does the encryption engine reside? Response:

- A. At the application using the database
- B. On the instance(s) attached to the volume
- C. In a key management system
- D. Within the database

**Answer:** D

#### NEW QUESTION 90

- (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 93

- (Exam Topic 2)

Which cloud service category brings with it the most expensive startup costs, but also the lowest costs for ongoing support and maintenance staff? Response:

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

**Answer:** B

#### NEW QUESTION 94

- (Exam Topic 2)

Which of the following is the best example of a key component of regulated PII? Response:



- A. Items that should be implemented
- B. Mandatory breach reporting
- C. Audit rights of subcontractors
- D. PCI DSS

**Answer:** B

#### NEW QUESTION 97

- (Exam Topic 2)

Penetration testing is a(n) \_\_\_\_\_ form of security assessment.

Response:

- A. Active
- B. Comprehensive
- C. Total
- D. Inexpensive

**Answer:** A

#### NEW QUESTION 99

- (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 102

- (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 104

- (Exam Topic 2)

Which type of cloud service category would having a vendor-neutral encryption scheme for data at rest (DAR) be the MOST important?

Response:

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

**Answer:** B

#### NEW QUESTION 108

- (Exam Topic 2)

You are the security director for a chain of automotive repair centers across several states. Your company uses a cloud SaaS provider, for business functions that cross several of the locations of your facilities, such as: 1) ordering parts 2) logistics and inventory 3) billing, and 4) marketing.

The manager at one of your newest locations reports that there is a competing car repair company that has a logo that looks almost exactly like the one your company uses. What will most likely affect the determination of who has ownership of the logo?

Response:

- A. Whoever first used the logo
- B. The jurisdiction where both businesses are using the logo simultaneously
- C. Whoever first applied for legal protection of the logo
- D. Whichever entity has the most customers that recognize the logo

**Answer:** C

#### NEW QUESTION 111

- (Exam Topic 2)

Which one of the following is not one of the three common threat modeling techniques? Response:

- A. Focused on assets
- B. Focused on attackers
- C. Focused on software
- D. Focused on social engineering

**Answer:** D

#### **NEW QUESTION 113**

- (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 117**

- (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 119**

- (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 124**

- (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 126**

- (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 129**

- (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 131

- (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 134

- (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 139

- (Exam Topic 2)

SOC 2 reports were intended to be \_\_\_\_\_.

Response:

- A. Released to the public
- B. Only technical assessments
- C. Retained for internal use
- D. Nonbinding

**Answer: C**

#### NEW QUESTION 144

- (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 147

- (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 149

- (Exam Topic 2)

What are the four cloud deployment models? Response:

- A. Public, Internal, Hybrid, and Community
- B. External, Private, Hybrid, and Community
- C. Public, Private, Joint, and Community
- D. Public, Private, Hybrid, and Community

**Answer: D**

#### NEW QUESTION 151

- (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 153

- (Exam Topic 2)

Data transformation in a cloud environment should be of great concern to organizations considering cloud migration because \_\_\_\_\_ could affect data classification processes/implementations.

Response:

- A. Multitenancy
- B. Virtualization
- C. Remote access
- D. Physical distance

**Answer: B**

#### NEW QUESTION 157

- (Exam Topic 2)

What is a cloud storage architecture that manages the data in a hierarchy of files? Response:

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

**Answer: B**

#### NEW QUESTION 159

- (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 163

- (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 164

- (Exam Topic 2)

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 168

- (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 171

- (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 174

- (Exam Topic 2)

Federation should be \_\_\_\_\_ to the users.

Response:

- A. Hostile
- B. Proportional
- C. Transparent
- D. Expensive

**Answer: C**

#### NEW QUESTION 179

- (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 182

- (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 183

- (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 186

- (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 187

- (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 189

- (Exam Topic 2)

\_\_\_\_\_ can often be the result of inadvertent activity. Response:

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

**Answer: C**

#### NEW QUESTION 190

- (Exam Topic 2)

Your organization is developing software for wide use by the public. You have decided to test it in a cloud environment, in a PaaS model. Which of the following should be of particular concern to your organization for this situation?

Response:

- A. Vendor lock-in
- B. Backdoors
- C. Regulatory compliance
- D. High-speed network connectivity

**Answer: B**

#### NEW QUESTION 194

- (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 197

- (Exam Topic 2)

Designers making applications for the cloud have to take into consideration risks and operational constraints that did not exist or were not as pronounced in the legacy environment.

Which of the following is an element cloud app designers may have to consider incorporating in software for the cloud that might not have been as important in the legacy environment?

Response:

- A. IAM capability
- B. DDoS resistance
- C. Encryption for data at rest and in motion
- D. Field validation

**Answer: C**

#### NEW QUESTION 200

- (Exam Topic 3)

Cloud vendors are held to contractual obligations with specified metrics by:

Response:

- A. SLAs
- B. Regulations
- C. Law
- D. Discipline

**Answer: A**

#### NEW QUESTION 201

- (Exam Topic 3)

Which technology is most associated with tunneling? Response:

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

**Answer:** B

#### NEW QUESTION 205

- (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 207

- (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 208

- (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 212

- (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 214

- (Exam Topic 3)

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

Response:

- A. Advanced persistent threats
- B. Account hijacking
- C. Malicious insiders
- D. Denial of service

**Answer:** C

#### NEW QUESTION 216

- (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 218

- (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 219

- (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 223

- (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 225

- (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 226

- (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 228

- (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 231

- (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 236

- (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 239

- (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 244

- (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 247

- (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 248

- (Exam Topic 3)

All of these are reasons an organization may want to consider cloud migration except: Response:

- A. Reduced personnel costs
- B. Elimination of risks
- C. Reduced operational expenses
- D. Increased efficiency

**Answer:** B

#### NEW QUESTION 249

- (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 253

- (Exam Topic 3)

Anonymization is the process of removing from data sets. Response:

- A. Access
- B. Cryptographic keys
- C. Numeric values
- D. Identifying information

**Answer:** D

#### NEW QUESTION 254

- (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 257

- (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 258

- (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 260

- (Exam Topic 3)

You are the security manager for a small surgical center. Your organization is reviewing upgrade options for its current, on-premises data center. In order to best meet your needs, which one of the following options would you recommend to senior management?

Response:

- A. Building a completely new data center
- B. Leasing a data center that is currently owned by another firm
- C. Renting private cloud space in a Tier 2 data center
- D. Staying with the current data center

**Answer:** A

#### NEW QUESTION 261

- (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 266**

- (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 268**

- (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 269**

- (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 274**

- (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 279**

- (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 280**

- (Exam Topic 3)

Bob is staging an attack against Alice's website. He is able to embed a link on her site that will execute malicious code on a visitor's machine, if the visitor clicks on the link. This is an example of which type of attack?

Response:

- A. Cross-site scripting
- B. Broken authentication/session management
- C. Security misconfiguration
- D. Insecure cryptographic storage

**Answer:** A

**NEW QUESTION 281**

.....

## Relate Links

**100% Pass Your CCSP Exam with Examible Prep Materials**

<https://www.examible.com/CCSP-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.examible.com/>