



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)

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 2

- (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 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)

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

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

Answer: C

NEW QUESTION 8

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 9

- (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 10

- (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 10

- (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 11

- (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 16

- (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 19

- (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 23

- (Exam Topic 1)

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

Response:

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

Answer: D

NEW QUESTION 24

- (Exam Topic 1)

_____ is the legal concept whereby a cloud customer is held to a reasonable expectation for providing security of its users' and clients' privacy data in their control.

Response:

- A. Due care
- B. Due diligence
- C. Liability
- D. Reciprocity

Answer: B

NEW QUESTION 27

- (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 30

- (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 33

- (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 36

- (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 37

- (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 38

- (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 39

- (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 40

- (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 41

- (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 43

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 44

- (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 47

- (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 50

- (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 52

- (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 57

- (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 61

- (Exam Topic 1)

Which of the following top security threats involves attempting to send invalid commands to an application in an attempt to get the application to execute the code?

Response:

- A. Cross-site scripting
- B. Injection
- C. Insecure direct object references
- D. Cross-site request forgery

Answer: B

NEW QUESTION 62

- (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 "sensitive data exposure."

Which of these is a technique to reduce the potential for a sensitive data exposure? Response:

- A. Extensive user training on proper data handling techniques
- B. Advanced firewalls inspecting all inbound traffic, to include content-based screening
- C. Ensuring the use of utility backup power supplies
- D. Roving security guards

Answer: A

NEW QUESTION 67

- (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 71

- (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 75

- (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 80

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 85

- (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 86

- (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 89

- (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 93

- (Exam Topic 1)

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 96

- (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 98

- (Exam Topic 1)

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

Response:

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

Answer: B

NEW QUESTION 102

- (Exam Topic 1)

Which of the following best describes a cloud carrier?

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

Answer: B

NEW QUESTION 103

- (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 104

- (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 106

- (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 109

- (Exam Topic 2)

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

- A. Mapping to existing access control lists (ACLs)
- B. Delineating biometric catalogs
- C. Preventing multifactor authentication
- D. Prohibiting unauthorized transposition

Answer: A

NEW QUESTION 114

- (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 118

- (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 121

- (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 122

- (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 124

- (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 128

- (Exam Topic 2)

A bare-metal hypervisor is Type _____.

Response:

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

Answer: A

NEW QUESTION 131

- (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 132

- (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 136

- (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 139

- (Exam Topic 2)

Which of the following methods is often used to obscure data from production systems for use in test or development environments?

Response:

- A. Tokenization
- B. Encryption
- C. Masking
- D. Classification

Answer: C

NEW QUESTION 141

- (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 145

- (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 148

- (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 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 154

- (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 156

- (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 159

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 161

- (Exam Topic 2)

In application-level encryption, where does the encryption engine reside? Response:

- A. In the application accessing the database
- B. In the OS on which the application is run
- C. Within the database accessed by the application
- D. In the volume where the database resides

Answer: A

NEW QUESTION 164

- (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 165

- (Exam Topic 2)

You are the security manager for a company that is considering cloud migration to an IaaS environment. You are assisting your company's IT architects in constructing the environment. Which of the following options do you recommend?

Response:

- A. Unrestricted public access
- B. Use of a Type I hypervisor
- C. Use of a Type II hypervisor
- D. Enhanced productivity without encryption

Answer: B

NEW QUESTION 170

- (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 175

- (Exam Topic 2)

Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?

Response:

- A. Systems
- B. Data
- C. Cash
- D. Personnel

Answer: C

NEW QUESTION 178

- (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)

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 181

- (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 183

- (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 187

- (Exam Topic 2)

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

Response:

- A. Regulatory oversight
- B. Financial penalties
- C. Performance details
- D. Desire to maintain customer satisfaction

Answer: B

NEW QUESTION 189

- (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 194

- (Exam Topic 2)

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

Response:

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

Answer: D

NEW QUESTION 198

- (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 201

- (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 202

- (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 205

- (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 208

- (Exam Topic 2)

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

Response:

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

Answer: B

NEW QUESTION 213

- (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)

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

Response:

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

Answer: D

NEW QUESTION 221

- (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 223

- (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 224

- (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 226

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 227

- (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 230

- (Exam Topic 3)

A user signs on to a cloud-based social media platform. In another browser tab, the user finds an article worth posting to the social media platform. The user clicks on the platform's icon listed on the article's website, and the article is automatically posted to the user's account on the social media platform.

This is an example of what?

Response:

- A. Single sign-on
- B. Insecure direct identifiers
- C. Identity federation
- D. Cross-site scripting

Answer: C

NEW QUESTION 234

- (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 235

- (Exam Topic 3)

In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?

Response:

- A. Technological
- B. Physical
- C. Administrative
- D. All of the above

Answer: D

NEW QUESTION 239

- (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 241

- (Exam Topic 3)

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

Response:

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

Answer: B

NEW QUESTION 245

- (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 246

- (Exam Topic 3)

During the assessment phase of a risk evaluation, what are the two types of tests that are performed? Response:

- A. Internal and external
- B. Technical and managerial
- C. Physical and logical
- D. Qualitative and quantitative

Answer: D

NEW QUESTION 250

- (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 252

- (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 255

- (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 258

- (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 259

- (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 261

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 265

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 270

- (Exam Topic 3)

With data in transit, which of the following will be the MOST major concern in order for a DLP solution to properly work?

Response:

- A. Scalability
- B. Encryption
- C. Redundancy
- D. Integrity

Answer: B

NEW QUESTION 271

- (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 272

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 274

- (Exam Topic 3)

The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "injection."

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

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

Answer: C

NEW QUESTION 275

- (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 278

- (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 282

- (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 287

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 292

- (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 293

- (Exam Topic 3)

Which of the following is not a security concern related to archiving data for long-term storage? Response:

- A. Long-term storage of the related cryptographic keys
- B. Format of the data
- C. Media the data resides on
- D. Underground depth of the storage facility

Answer: D

NEW QUESTION 297

- (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 302

- (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 304

- (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 308

- (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 309

- (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 313

- (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 315

- (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 317

- (Exam Topic 3)

What is one of the benefits of implementing an egress monitoring solution? Response:

- A. Preventing DDoS attacks
- B. Inventorying data assets
- C. Interviewing data owners
- D. Protecting against natural disasters

Answer: B

NEW QUESTION 322

- (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 325

- (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 329

- (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 332

.....

Relate Links

100% Pass Your CCSP Exam with ExamBible Prep Materials

<https://www.exambible.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.exambible.com/>