ISC2

Exam Questions CCSP

Certified Cloud Security Professional

NEW QUESTION 1
- (Exam Topic 1)
_____ can often be the result of inadvertent activity. Response:

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

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
What is the term that describes the situation when a malicious user/attacker can exit the restrictions of a single host and access other nodes on the network? Response:

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

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
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 4
- (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 5
- (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 6
- (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 7
- (Exam Topic 1)
What is the federal agency that accepts applications for new patents?

A. USDA
B. USPTO
C. OSHA

D. SEC

Answer: B

NEW QUESTION 8
- (Exam Topic 1)
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 9
- (Exam Topic 1)
Which document will enforce uptime and availability requirements between the cloud customer and cloud provider?
Response:

A. Contract
B. Operational level agreement
C. Service level agreement
D. Regulation

Answer: C

NEW QUESTION 10
- (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 10
- (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 11
- (Exam Topic 1)
You are the security policy lead for your organization, which is considering migrating from your
on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization. Which of the following benefits will the CSA CCM offer your organization? Response:

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

Answer: A

NEW QUESTION 14
- (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 15
- (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, who initiates the protocol?
Response:

A. The server
B. The client
C. The certifying authority
D. The ISP

Answer: B

NEW QUESTION 17
- (Exam Topic 1)
Which of the following tools might be useful in data discovery efforts that are based on content analysis?

A. DLP
B. Digital Rights Management (DRM)
C. iSCSI
D. Fibre Channel over Ethernet (FCoE)

Answer: A

NEW QUESTION 18
- (Exam Topic 1)
Because PaaS implementations are so often used for software development, what is one of the vulnerabilities that should always be kept in mind?
Response:

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

Answer: C

NEW QUESTION 19
- (Exam Topic 1)
Which of the following is considered an administrative control?

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

Answer: A

NEW QUESTION 22
- (Exam Topic 1)
Who is ultimately responsible for a data breach that includes personally identifiable information (PII), in the event of negligence on the part of the cloud provider?

A. The user
B. The subject
C. The cloud provider
D. The cloud customer

Answer: D

NEW QUESTION 27
- (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 31
- (Exam Topic 1)
Which of the following is the recommended operating range for temperature and humidity in a data center?
Response:

A. Between 62 °F - 81 °F and 40% and 65% relative humidity
B. Between 64 °F - 81 °F and 40% and 60% relative humidity
C. Between 64 °F - 84 °F and 30% and 60% relative humidity

D. Between 60 °F - 85 °F and 40% and 60% relative humidity

Answer: B

NEW QUESTION 35
- (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 36
- (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 37
- (Exam Topic 1)
The final phase of the cloud data lifecycle is the destroy phase, where data is ultimately deleted and done so in a secure manner to ensure it cannot be recovered or reconstructed. Which cloud service category poses the most challenges to data destruction or the cloud customer?

A. Platform
B. Software
C. Infrastructure
D. Desktop

Answer: B

NEW QUESTION 38
- (Exam Topic 1)
Which Common Criteria Evaluation Assurance Level (EAL) is granted to those products that are formally verified in terms of design and tested by an independent third party?

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

Answer: D

NEW QUESTION 39
- (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 40
- (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 43
- (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 47
- (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 49
- (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 53
- (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 55
- (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 57
- (Exam Topic 1)
Using one cloud provider for your operational environment and another for your BCDR backup will also give you the additional benefit of _____.
Response:

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

Answer: B

NEW QUESTION 61
- (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 63
- (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 65
- (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 68
- (Exam Topic 1)
DRM solutions should generally include all the following functions, except:

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

Answer: B

NEW QUESTION 73
- (Exam Topic 1)
Static software security testing typically uses _____ as a measure of how thorough the testing was. Response:

A. Number of testers
B. Flaws detected
C. Code coverage
D. Malware hits

Answer: C

NEW QUESTION 74
- (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 79
- (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 84

- (Exam Topic 1)
Application virtualization can typically be used for .

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

Answer: D

NEW QUESTION 88
- (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 92
- (Exam Topic 1)
Heating, ventilation, and air conditioning (HVAC) systems cool the data center by pushing warm air into _____.
Response:

A. The server inlets
B. Underfloor plenums
C. HVAC intakes
D. The outside world

Answer: D

NEW QUESTION 96
- (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 98
- (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 99
- (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 103
- (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 107
- (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 109
- (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 112
- (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 115
- (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 116
- (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 117
- (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 122
- (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 124
- (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 126
- (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 129
- (Exam Topic 2)
A bare-metal hypervisor is Type _____.
Response:

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

Answer: A

NEW QUESTION 133
- (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 134
- (Exam Topic 2)
Which key storage solution would be the BEST choice in a situation where availability might be of a particular concern?
Response:

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

Answer: A

NEW QUESTION 135
- (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 139
- (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 144
- (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 149
- (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 153
- (Exam Topic 2)
Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?
Response:

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

Answer: A

NEW QUESTION 154
- (Exam Topic 2)
Which of the following is NOT a core component of an SIEM solution? Response:

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

Answer: D

NEW QUESTION 159
- (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 161

- (Exam Topic 2)
An organization could have many reasons that are common throughout the industry to activate a BCDR situation. Which of the following is NOT a typical reason to activate a BCDR plan?
Response:

A. Natural disaster
B. Utility outage
C. Staff loss
D. Terrorist attack

Answer: C

NEW QUESTION 166
- (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 169
- (Exam Topic 2)
Which of the following would NOT be included as input into the requirements gathering for an application or system?
Response:

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

Answer: D

NEW QUESTION 174
- (Exam Topic 2)
Why does the physical location of your data backup and/or BCDR failover environment matter? Response:

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

Answer: A

NEW QUESTION 175
- (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 178
- (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 182
- (Exam Topic 2)
Which of the following is the correct name for Tier II of the Uptime Institute Data Center Site Infrastructure Tier Standard Topology?

Response:

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

Answer: D

NEW QUESTION 185
- (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 189
- (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 191
- (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 195
- (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 198
- (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 202
- (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 205
- (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 209
- (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 214
- (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 217
- (Exam Topic 2)
When designing a cloud data center, which of the following aspects is not necessary to ensure continuity of operations during contingency operations?
Response:

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

Answer: C

NEW QUESTION 219
- (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 220
- (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 224
- (Exam Topic 2)
Aside from the fact that the cloud customer probably cannot locate/reach the physical storage assets of the cloud provider, and that wiping an entire storage space

would impact other customers, why would degaussing probably not be an effective means of secure sanitization in the cloud?
Response:

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

Answer: B

NEW QUESTION 228
- (Exam Topic 2)
Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality? Response:

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

Answer: C

NEW QUESTION 230
- (Exam Topic 2)
The tasks performed by the hypervisor in the virtual environment can most be likened to the tasks of the
_____ in the legacy environment.
Response:

A. Central processing unit (CPU)
B. Security team
C. OS
D. PGP

Answer: A

NEW QUESTION 234
- (Exam Topic 2)
From a security perspective, automation of configuration aids in _____.
Response:

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

Answer: B

NEW QUESTION 235
- (Exam Topic 3)
Why might an organization choose to comply with the ISO 27001 standard?
Response:

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

Answer: C

NEW QUESTION 240
- (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 244
- (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 245
- (Exam Topic 3)
Which technology is most associated with tunneling? Response:

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

Answer: B

NEW QUESTION 249
- (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 252
- (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 254
- (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 256
- (Exam Topic 3)
Which of the following aspects of the BC/DR process poses a risk to the organization? Response:

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

Answer: D

NEW QUESTION 257
- (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 258

- (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 262
- (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 267
- (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 272
- (Exam Topic 3)
When a customer performs a penetration test in the cloud, why isn't the test an optimum simu-lation 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 276
- (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 277
- (Exam Topic 3)
A loosely coupled storage cluster will have performance and capacity limitations based on the _____.
Response:

A. Physical backplane connecting it
B. Total number of nodes in the cluster
C. Amount of usage demanded
D. The performance and capacity in each node

Answer: D

NEW QUESTION 281
- (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 285
- (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 287
- (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 290
- (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 295
- (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 297
- (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 302
- (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 307
- (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 310
- (Exam Topic 3)
Dynamic application security testing (DAST) is usually considered a _____ form of testing. Response:
White-box

A. Parched field
B. Black-box
C. Gray-box
D. Parched field

Answer: B

NEW QUESTION 315
- (Exam Topic 3)
Which type of web application monitoring most closely measures actual activity? Response:

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

Answer: B

NEW QUESTION 318
- (Exam Topic 3)
Which of the following methods of addressing risk is most associated with insurance? Response:

A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

Answer: A

NEW QUESTION 323
- (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 327
- (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 330
- (Exam Topic 3)
Which is the most commonly used standard for information exchange within a federated identity system? Response:

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

Answer: C

NEW QUESTION 333
- (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 334
- (Exam Topic 3)
In which of the following situations does the data owner have to administer the OS? Response:

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

Answer: A

NEW QUESTION 339
- (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 344
- (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 345
- (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 346
- (Exam Topic 3)
Which of the following is perhaps the best method for reducing the risk of a specific application not delivering the proper level of functionality and performance when it is moved from the legacy environment into the cloud?
Response:

A. Remove the application from the organization's production environment, and replace it with something else.

B. Negotiate and conduct a trial run in the cloud environment for that application before permanently migrating.
C. Make sure the application is fully updated and patched according to all vendor specifications.
D. Run the application in an emulator.

Answer: B

NEW QUESTION 349
......

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

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

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
What is the term that describes the situation when a malicious user/attacker can exit the restrictions of a single host and access other nodes on the network? Response:

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

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
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 4
- (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 5
- (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 6
- (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 7
- (Exam Topic 1)
What is the federal agency that accepts applications for new patents?

A. USDA
B. USPTO
C. OSHA

D. SEC

Answer: B

NEW QUESTION 8
- (Exam Topic 1)
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 9
- (Exam Topic 1)
Which document will enforce uptime and availability requirements between the cloud customer and cloud provider?
Response:

A. Contract
B. Operational level agreement
C. Service level agreement
D. Regulation

Answer: C

NEW QUESTION 10
- (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 10
- (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 11
- (Exam Topic 1)
You are the security policy lead for your organization, which is considering migrating from your
on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization. Which of the following benefits will the CSA CCM offer your organization? Response:

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

Answer: A

NEW QUESTION 14
- (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 15
- (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, who initiates the protocol?
Response:

A. The server
B. The client
C. The certifying authority
D. The ISP

Answer: B

NEW QUESTION 17
- (Exam Topic 1)
Which of the following tools might be useful in data discovery efforts that are based on content analysis?

A. DLP
B. Digital Rights Management (DRM)
C. iSCSI
D. Fibre Channel over Ethernet (FCoE)

Answer: A

NEW QUESTION 18
- (Exam Topic 1)
Because PaaS implementations are so often used for software development, what is one of the vulnerabilities that should always be kept in mind?
Response:

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

Answer: C

NEW QUESTION 19
- (Exam Topic 1)
Which of the following is considered an administrative control?

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

Answer: A

NEW QUESTION 22
- (Exam Topic 1)
Who is ultimately responsible for a data breach that includes personally identifiable information (PII), in the event of negligence on the part of the cloud provider?

A. The user
B. The subject
C. The cloud provider
D. The cloud customer

Answer: D

NEW QUESTION 27
- (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 31
- (Exam Topic 1)
Which of the following is the recommended operating range for temperature and humidity in a data center?
Response:

A. Between 62 °F - 81 °F and 40% and 65% relative humidity
B. Between 64 °F - 81 °F and 40% and 60% relative humidity
C. Between 64 °F - 84 °F and 30% and 60% relative humidity

D. Between 60 °F - 85 °F and 40% and 60% relative humidity

Answer: B

NEW QUESTION 35
- (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 36
- (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 37
- (Exam Topic 1)
The final phase of the cloud data lifecycle is the destroy phase, where data is ultimately deleted and done so in a secure manner to ensure it cannot be recovered or reconstructed. Which cloud service category poses the most challenges to data destruction or the cloud customer?

A. Platform
B. Software
C. Infrastructure
D. Desktop

Answer: B

NEW QUESTION 38
- (Exam Topic 1)
Which Common Criteria Evaluation Assurance Level (EAL) is granted to those products that are formally verified in terms of design and tested by an independent third party?

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

Answer: D

NEW QUESTION 39
- (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 40
- (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 43
- (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 47
- (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 49
- (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 53
- (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 55
- (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 57
- (Exam Topic 1)
Using one cloud provider for your operational environment and another for your BCDR backup will also give you the additional benefit of _____.
Response:

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

Answer: B

NEW QUESTION 61
- (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 63
- (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 65
- (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 68
- (Exam Topic 1)
DRM solutions should generally include all the following functions, except:

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

Answer: B

NEW QUESTION 73
- (Exam Topic 1)
Static software security testing typically uses _____ as a measure of how thorough the testing was. Response:

A. Number of testers
B. Flaws detected
C. Code coverage
D. Malware hits

Answer: C

NEW QUESTION 74
- (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 79
- (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 84

- (Exam Topic 1)
Application virtualization can typically be used for .

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

Answer: D

NEW QUESTION 88
- (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 92
- (Exam Topic 1)
Heating, ventilation, and air conditioning (HVAC) systems cool the data center by pushing warm air into _____.
Response:

A. The server inlets
B. Underfloor plenums
C. HVAC intakes
D. The outside world

Answer: D

NEW QUESTION 96
- (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 98
- (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 99
- (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 103
- (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 107
- (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 109
- (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 112
- (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 115
- (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 116
- (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 117
- (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 122
- (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 124
- (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 126
- (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 129
- (Exam Topic 2)
A bare-metal hypervisor is Type _____.
Response:

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

Answer: A

NEW QUESTION 133
- (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 134
- (Exam Topic 2)
Which key storage solution would be the BEST choice in a situation where availability might be of a particular concern?
Response:

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

Answer: A

NEW QUESTION 135
- (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 139
- (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 144
- (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 149
- (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 153
- (Exam Topic 2)
Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?
Response:

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

Answer: A

NEW QUESTION 154
- (Exam Topic 2)
Which of the following is NOT a core component of an SIEM solution? Response:

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

Answer: D

NEW QUESTION 159
- (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 161

- (Exam Topic 2)
An organization could have many reasons that are common throughout the industry to activate a BCDR situation. Which of the following is NOT a typical reason to activate a BCDR plan?
Response:

A. Natural disaster
B. Utility outage
C. Staff loss
D. Terrorist attack

Answer: C

NEW QUESTION 166
- (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 169
- (Exam Topic 2)
Which of the following would NOT be included as input into the requirements gathering for an application or system?
Response:

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

Answer: D

NEW QUESTION 174
- (Exam Topic 2)
Why does the physical location of your data backup and/or BCDR failover environment matter? Response:

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

Answer: A

NEW QUESTION 175
- (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 178
- (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 182
- (Exam Topic 2)
Which of the following is the correct name for Tier II of the Uptime Institute Data Center Site Infrastructure Tier Standard Topology?

Response:

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

Answer: D

NEW QUESTION 185
- (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 189
- (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 191
- (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 195
- (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 198
- (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 202
- (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 205
- (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 209
- (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 214
- (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 217
- (Exam Topic 2)
When designing a cloud data center, which of the following aspects is not necessary to ensure continuity of operations during contingency operations?
Response:

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

Answer: C

NEW QUESTION 219
- (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 220
- (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 224
- (Exam Topic 2)
Aside from the fact that the cloud customer probably cannot locate/reach the physical storage assets of the cloud provider, and that wiping an entire storage space

would impact other customers, why would degaussing probably not be an effective means of secure sanitization in the cloud?
Response:

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

Answer: B

NEW QUESTION 228
- (Exam Topic 2)
Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality? Response:

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

Answer: C

NEW QUESTION 230
- (Exam Topic 2)
The tasks performed by the hypervisor in the virtual environment can most be likened to the tasks of the
_____ in the legacy environment.
Response:

A. Central processing unit (CPU)
B. Security team
C. OS
D. PGP

Answer: A

NEW QUESTION 234
- (Exam Topic 2)
From a security perspective, automation of configuration aids in _____.
Response:

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

Answer: B

NEW QUESTION 235
- (Exam Topic 3)
Why might an organization choose to comply with the ISO 27001 standard?
Response:

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

Answer: C

NEW QUESTION 240
- (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 244
- (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 245
- (Exam Topic 3)
Which technology is most associated with tunneling? Response:

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

Answer: B

NEW QUESTION 249
- (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 252
- (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 254
- (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 256
- (Exam Topic 3)
Which of the following aspects of the BC/DR process poses a risk to the organization? Response:

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

Answer: D

NEW QUESTION 257
- (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 258

- (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 262
- (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 267
- (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 272
- (Exam Topic 3)
When a customer performs a penetration test in the cloud, why isn't the test an optimum simu-lation 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 276
- (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 277
- (Exam Topic 3)
A loosely coupled storage cluster will have performance and capacity limitations based on the _____.
Response:

A. Physical backplane connecting it
B. Total number of nodes in the cluster
C. Amount of usage demanded
D. The performance and capacity in each node

Answer: D

NEW QUESTION 281
- (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 285
- (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 287
- (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 290
- (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 295
- (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 297
- (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 302
- (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 307
- (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 310
- (Exam Topic 3)
Dynamic application security testing (DAST) is usually considered a _____ form of testing. Response:
White-box

A. Parched field
B. Black-box
C. Gray-box
D. Parched field

Answer: B

NEW QUESTION 315
- (Exam Topic 3)
Which type of web application monitoring most closely measures actual activity? Response:

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

Answer: B

NEW QUESTION 318
- (Exam Topic 3)
Which of the following methods of addressing risk is most associated with insurance? Response:

A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

Answer: A

NEW QUESTION 323
- (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 327
- (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 330
- (Exam Topic 3)
Which is the most commonly used standard for information exchange within a federated identity system? Response:

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

Answer: C

NEW QUESTION 333
- (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 334
- (Exam Topic 3)
In which of the following situations does the data owner have to administer the OS? Response:

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

Answer: A

NEW QUESTION 339
- (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 344
- (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 345
- (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 346
- (Exam Topic 3)
Which of the following is perhaps the best method for reducing the risk of a specific application not delivering the proper level of functionality and performance when it is moved from the legacy environment into the cloud?
Response:

A. Remove the application from the organization's production environment, and replace it with something else.

B. Negotiate and conduct a trial run in the cloud environment for that application before permanently migrating.
C. Make sure the application is fully updated and patched according to all vendor specifications.
D. Run the application in an emulator.

Answer: B

NEW QUESTION 349
......

B. Negotiate and conduct a trial run in the cloud environment for that application before permanently migrating.
C. Make sure the application is fully updated and patched according to all vendor specifications.
D. Run the application in an emulator.

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/