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) What can tokenization be used for? Response:

A. Encryption
B. Compliance with PCI DSS
C. Enhancing the user experience
D. Giving management oversight to e-commerce functions

Answer: B

NEW QUESTION 4
- (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 5
- (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 6
- (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 7
- (Exam Topic 1)
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing? Response:

A. Cloud customers and third parties are continually enhancing and modifying APIs.
B. APIs can have automated settings.

C. It is impossible to uninstall APIs.
D. APIs are a form of malware.

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
What type of device is often leveraged to assist legacy applications that may not have the programmatic capability to process assertions from modern web services?

A. Web application firewall
B. XML accelerator
C. Relying party
D. XML firewall

Answer: B

NEW QUESTION 9
- (Exam Topic 1)
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “unvalidated redirects and forwards.”
Which of the following is a good way to protect against this problem? Response:

A. Don’t use redirects/forwards in your applications.
B. Refrain from storing credentials long term.
C. Implement security incident/event monitoring (security information and event management (SIEM)/security information management (SIM)/security event management (SEM)) solutions.
D. Implement digital rights management (DRM) solutions.

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
When an organization implements an SIEM solution and begins aggregating event data, the configured event sources are only valid at the time it was configured. Application modifications, patching, and other upgrades will change the events generated and how they are represented over time.
What process is necessary to ensure events are collected and processed with this in mind?

A. Continual review
B. Continuous optimization
C. Aggregation updates
D. Event elasticity

Answer: B

NEW QUESTION 10
- (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 14
- (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 17
- (Exam Topic 1)
Which of the following best describes SAML? Response:

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

Answer: B

NEW QUESTION 20
- (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 21
- (Exam Topic 1)
A typical DLP tool can enhance the organization's efforts at accomplishing what legal task? Response:

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

Answer: A

NEW QUESTION 23
- (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 28
- (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 31
- (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 34
- (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 38

- (Exam Topic 1)
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.
If you don't use cross-certification, what other model can you implement for this purpose? Response:

A. Third-party identity broker
B. Cloud reseller
C. Intractable nuanced variance
D. Mandatory access control (MAC)

Answer: A

NEW QUESTION 41
- (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 45
- (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 50
- (Exam Topic 1)
Cloud environments pose many unique challenges for a data custodian to properly adhere to policies and the use of data. What poses the biggest challenge for a data custodian with a PaaS implementation, over and above the same concerns with IaaS?
Response:

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

Answer: B

NEW QUESTION 53
- (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 54
- (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 57
- (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 60
- (Exam Topic 1)
Different types of cloud deployment models use different types of storage from traditional data centers, along with many new types of software platforms for deploying applications and configurations. Which of the following is NOT a storage type used within a cloud environment?

A. Docker
B. Object
C. Structured
D. Volume

Answer: A

NEW QUESTION 63
- (Exam Topic 1)
In the cloud motif, the data processor is usually: Response:

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

Answer: C

NEW QUESTION 64
- (Exam Topic 1)
Why are PaaS environments at a higher likelihood of suffering backdoor vulnerabilities?

A. They rely on virtualization.
B. They are often used for software development.
C. They have multitenancy.
D. They are scalable.

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
Which of the following is the correct name for Tier II of the Uptime Institute Data Center Site Infrastructure Tier Standard Topology?

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

Answer: D

NEW QUESTION 70
- (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 75
- (Exam Topic 1)
A firewall can use all of the following techniques for controlling traffic except:

A. Rule sets
B. Behavior analysis
C. Content filtering
D. Randomization

Answer: D

NEW QUESTION 76

- (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 79
- (Exam Topic 1)
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except: Response:

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

Answer: B

NEW QUESTION 81
- (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 85
- (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 90
- (Exam Topic 1) What does nonrepudiation mean? Response:

A. Prohibiting certain parties from a private conversation
B. Ensuring that a transaction is completed before saving the results
C. Ensuring that someone cannot turn off auditing capabilities while performing a function
D. Preventing any party that participates in a transaction from claiming that it did not

Answer: D

NEW QUESTION 95
- (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 96
- (Exam Topic 1)
Log data should be protected _____.
Response:

A. One level below the sensitivity level of the systems from which it was collected
B. At least at the same sensitivity level as the systems from which it was collected

C. With encryption in transit, at rest, and in use
D. According to NIST guidelines

Answer: B

NEW QUESTION 100
- (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 104
- (Exam Topic 1)
Who is the entity identified by personal data? Response:

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

Answer: D

NEW QUESTION 106
- (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 107
- (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 109
- (Exam Topic 1)
SOX was enacted because of which of the following? Response:

A. Poor BOD oversight
B. Lack of independent audits
C. Poor financial controls
D. All of the above

Answer: D

NEW QUESTION 113
- (Exam Topic 1)
A honeypot should contain data_____.
Response:

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

Answer: C

NEW QUESTION 114

- (Exam Topic 1)
Who should be the only entity allowed to declare that an organization can return to normal following contingency or BCDR operations?
Response:

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

Answer: D

NEW QUESTION 115
- (Exam Topic 1)
Which of the following management risks can make an organization’s cloud environment unviable? Response:

A. Insider trading
B. VM sprawl
C. Hostile takeover
D. Improper personnel selection

Answer: B

NEW QUESTION 117
- (Exam Topic 1)
Which of the following is not a reason for conducting audits?

A. Regulatory compliance
B. User satisfaction
C. Determination of service quality
D. Security assurance

Answer: B

NEW QUESTION 118
- (Exam Topic 1)
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
In order to increase the security value of the DLP, you should consider combining it with _____.
Response:

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

Answer: A

NEW QUESTION 123
- (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 124
- (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 129
- (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 131
- (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 136
- (Exam Topic 1)
What are the six components that make up the STRIDE threat model? Response:

A. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
B. Spoofing, Tampering, Non-Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
C. Spoofing, Tampering, Repudiation, Information Disclosure, Distributed Denial of Service, and Elevation of Privilege
D. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Social Engineering

Answer: A

NEW QUESTION 137
- (Exam Topic 1)
The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet). In a typical TLS session, what is the usual means for establishing trust between the parties?
Response:

A. Out-of-band authentication
B. Multifactor authentication
C. PKI certificates
D. Preexisting knowledge of each other

Answer: C

NEW QUESTION 139
- (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 144
- (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 148
- (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 151

- (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 154
- (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 155
- (Exam Topic 2)
Which type of cloud service category would having a vendor-neutral encryption scheme for data at rest (DAR) be the MOST important?
Response:

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

Answer: B

NEW QUESTION 157
- (Exam Topic 2)
A bare-metal hypervisor is Type _____.
Response:

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

Answer: A

NEW QUESTION 159
- (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 162
- (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 167

- (Exam Topic 2)
Your organization has made it a top priority that any cloud environment being considered to host production systems have guarantees that resources will always be available for allocation when needed.
Which of the following concepts will you need to ensure is part of the contract and SLA? Response:

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

Answer: D

NEW QUESTION 171
- (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 173
- (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 178
- (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. Persistence
B. Influence
C. Resistance
D. Trepidation

Answer: A

NEW QUESTION 181
- (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 183
- (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 188
- (Exam Topic 2)
Which of the following is NOT one of the cloud computing activities, as outlined in ISO/IEC 17789? Response:

A. Cloud service provider
B. Cloud service partner
C. Cloud service administrator
D. Cloud service customer

Answer: C

NEW QUESTION 192
- (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 197
- (Exam Topic 2)
A cloud data encryption situation where the cloud customer retains control of the encryption keys and the cloud provider only processes and stores the data could be considered a _____.
Response:

A. Threat
B. Risk
C. Hybrid cloud deployment model
D. Case of infringing on the rights of the provider

Answer: C

NEW QUESTION 198
- (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 200
- (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 201
- (Exam Topic 2)
Firewalls can detect attack traffic by using all these methods except _____.
Response:

A. Known past behavior in the environment
B. Identity of the malicious user
C. Point of origination
D. Signature matching

Answer: B

NEW QUESTION 203
- (Exam Topic 2)
All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline except _____.
Response:

A. Remove all nonessential programs from the baseline image
B. Exclude the target system you intend to baseline from any scheduled updates/patching used inproduction systems
C. Include the baseline image in the asset inventory/configuration management database

D. Configure the host OS according to the baseline requirements

Answer: C

NEW QUESTION 206
- (Exam Topic 2)
Before deploying a specific brand of virtualization toolset, it is important to configure it according to _____ .
Response:

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

Answer: C

NEW QUESTION 207
- (Exam Topic 2)
What is the most secure form of code testing and review? Response:

A. Open source
B. Proprietary/internal
C. Neither open source nor proprietary
D. Combination of open source and proprietary

Answer: D

NEW QUESTION 208
- (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 210
- (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 214
- (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 218
- (Exam Topic 2)
Tokenization requires at least _____ database(s).
Response:

A. One
B. Two
C. Three
D. Four

Answer: B

NEW QUESTION 220
- (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 224
- (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 229
- (Exam Topic 2)
In the cloud motif, the data processor is usually: Response:

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

Answer: C

NEW QUESTION 232
- (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 237
- (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 239
- (Exam Topic 2)
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “using components with known vulnerabilities.”
Why would an organization ever use components with known vulnerabilities to create software? Response:

A. The organization is insured.
B. The particular vulnerabilities only exist in a context not being used by developers.
C. Some vulnerabilities only exist in foreign countries.
D. A component might have a hidden vulnerability.

Answer: B

NEW QUESTION 244
- (Exam Topic 2)
According to OWASP recommendations, active software security testing should include all of the following except _____ .
Response:

A. Session initiation testing
B. Input validation testing
C. Testing for error handling
D. Testing for weak cryptography

Answer: A

NEW QUESTION 246
- (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 251
- (Exam Topic 2)
Each of the following is an element of the Identification phase of the identity and access management (IAM) process except _____.
Response:

A. Provisioning
B. Inversion
C. Management
D. Deprovisioning

Answer: B

NEW QUESTION 256
- (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 260
- (Exam Topic 2) What are SOCI/SOCII/SOCIII? Response:

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

Answer: C

NEW QUESTION 261
- (Exam Topic 2)
What type of software is often considered secured and validated via community knowledge?
Response:

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

Answer: C

NEW QUESTION 262
- (Exam Topic 2)
TLS provides _____ and _____ for communications. Response:

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

Answer: C

NEW QUESTION 263

- (Exam Topic 2)
Which phase of the cloud data lifecycle also typically entails the process of data classification? Response:

A. Use
B. Store
C. Create
D. Archive

Answer: C

NEW QUESTION 264
- (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 266
- (Exam Topic 2)
You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center.
One of the challenges you're facing is whether the provider will have undue control over your data once it is within the provider's data center; will the provider be able to hold your organization hostage because they have your data?
This is a(n) _____ issue. Response:

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

Answer: B

NEW QUESTION 267
- (Exam Topic 2)
Federation should be _____ to the users.
Response:

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

Answer: C

NEW QUESTION 270
- (Exam Topic 2)
Which type of report is considered for "general" use and does not contain any sensitive information? Response:

A. SOC 1
B. SAS-70
C. SOC 3
D. SOC 2

Answer: C

NEW QUESTION 272
- (Exam Topic 2)
You have been tasked by management to offload processing and validation of incoming encoded data from your application servers and their associated APIs.
Which of the following would be the most appropriate device or software to consider?
Response:

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

Answer: A

NEW QUESTION 274
- (Exam Topic 2)
Which of the following is a method for apportioning resources that involves prioritizing resource requests to resolve contention situations?
Response:

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

Answer: B

NEW QUESTION 277
- (Exam Topic 2)
An audit against the _____ will demonstrate that an organization has ¬adequate security controls to meet its ISO 27001 requirements.
Response:

A. SAS 70 standard
B. SSAE 16 standard
C. ISO 27002 certification criteria
D. NIST SP 800-53

Answer: C

NEW QUESTION 280
- (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 284
- (Exam Topic 2)
Which of the following data protection methodologies maintains the ability to connect back values to the original values?
Response:

A. Tokenization
B. Anonymization
C. Obfuscation
D. Dynamic mapping

Answer: A

NEW QUESTION 285
- (Exam Topic 2)
Which of these characteristics of a virtualized network adds risks to the cloud environment? Response:

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

Answer: A

NEW QUESTION 289
- (Exam Topic 2)
Which of the following is not a way to manage risk? Response:

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

Answer: A

NEW QUESTION 291
- (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 295
- (Exam Topic 3)
Federation allows _____ across organizations.
Response:

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

Answer: D

NEW QUESTION 300
- (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 301
- (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 305
- (Exam Topic 3)
Which of the following methods for the safe disposal of electronic records can always be used in a cloud environment? Response:

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

Answer: B

NEW QUESTION 309
- (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 311
- (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 313

- (Exam Topic 3)
The Brewer-Nash security model is also known as which of the following? Response:

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

Answer: B

NEW QUESTION 315
- (Exam Topic 3)
Access should be based on _____.
Response:

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

Answer: B

NEW QUESTION 320
- (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 323
- (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 324
- (Exam Topic 3)
A cloud provider is looking to provide a higher level of assurance to current and potential cloud customers about the design and effectiveness of their security controls.
Which of the following audit reports would the cloud provider choose as the most appropriate to accomplish this goal?
Response:

A. SAS-70
B. SOC 1
C. SOC 2
D. SOC 3

Answer: D

NEW QUESTION 329
- (Exam Topic 3)
Fiber-optic lines are considered part of layer _____ of the OSI model. Response:

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

Answer: A

NEW QUESTION 330
- (Exam Topic 3)
Digital rights management (DRM) tools can be combined with _____, to enhance security capabilities. Response:

A. Roaming identity services (RIS)
B. Egress monitoring solutions (DLP)
C. Internal hardware settings (BIOS)

D. Remote Authentication Dial-In User Service (RADIUS)

Answer: B

NEW QUESTION 331
- (Exam Topic 3)
Which of the following is not a component of the of the STRIDE model? Response:

A. Spoofing
B. Repudiation
C. Information disclosure
D. External pen testing

Answer: D

NEW QUESTION 335
- (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 336
- (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 339
- (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 342
- (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 347
- (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 348
- (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 352
- (Exam Topic 3)
When using an Infrastructure as a Service (IaaS) solution, what is the capability provided to the customer? Response:

A. To provision processing, storage, networks, and other fundamental computing resources when the consumer is not able to deploy and run arbitrary software, which can include operating systems and applications.
B. To provision processing, storage, networks, and other fundamental computing resources when the provider is able to deploy and run arbitrary software, which can include operating systems and applications.
C. To provision processing, storage, networks, and other fundamental computing resources when the auditor is able to deploy and run arbitrary software, which can include operating systems and applications.
D. To provision processing, storage, networks, and other fundamental computing resources when the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Answer: D

NEW QUESTION 355
- (Exam Topic 3)
FM-200 has all the following properties except _____.
Response:

A. It’s nontoxic at levels used for fire suppression
B. It’s gaseous at room temperature
C. It may deplete the Earth’s ozone layer
D. It does not leave a film or coagulant after use

Answer: C

NEW QUESTION 356
- (Exam Topic 3)
Which theoretical technology would allow superposition of physical states to increase both computing capacity and encryption keyspace?
Response:

A. All-or-nothing-transform with Reed-Solomon (AONT-RS)
B. Quantum computing
C. Filigree investment
D. Sharding

Answer: B

NEW QUESTION 359
- (Exam Topic 3)
Which of the following might make crypto-shredding difficult or useless? Response:

A. Cloud provider also managing the organization’s keys
B. Lack of physical access to the environment
C. External attackers
D. Lack of user training and awareness

Answer: A

NEW QUESTION 362
- (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 364
- (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 366
- (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 369
- (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 371
- (Exam Topic 3)
There are two reasons to conduct a test of the organization’s recovery from backup in an environment other than the primary production environment. Which of the following is one of them? Response:

A. It is good to invest in more than one community.
B. You want to approximate contingency conditions, which includes not operating in the primary location.
C. It is good for your personnel to see other places occasionally.
D. Your regulators won’t follow you offsite, so you’ll be unobserved during your test.

Answer: B

NEW QUESTION 375
- (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 380
- (Exam Topic 3)
Which characteristic of automated patching makes it attractive? Response:

A. Cost
B. Speed
C. Noise reduction
D. Capability to recognize problems quickly

Answer: B

NEW QUESTION 382
- (Exam Topic 3)
Your company operates in a highly competitive market, with extremely high-value data assets. Senior management wants to migrate to a cloud environment but is concerned that providers will not meet the company’s security needs.
Which deployment model would probably best suit the company’s needs? Response:

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

Answer: B

NEW QUESTION 386
- (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 388
- (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 393
- (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 395
- (Exam Topic 3)
In addition to BCDR, what other benefit can your data archive/backup provide? Response:

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

Answer: D

NEW QUESTION 398
- (Exam Topic 3)
Security best practices in a virtualized network environment would include which of the following? Response:

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

Answer: A

NEW QUESTION 401
- (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 405
- (Exam Topic 3)
What is the term used to describe loss of access to data because the cloud provider has ceased operation? Response:

A. Closing

B. Vendor lock-out
C. Vendor lock-in
D. Masking

Answer: B

NEW QUESTION 410
- (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 415
- (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 416
- (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 418
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CCSP Practice Exam Features:

* CCSP Questions and Answers Updated Frequently

* CCSP Practice Questions Verified by Expert Senior Certified Staff

* CCSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CCSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year