ISC2

Exam Questions CCSP

Certified Cloud Security Professional

NEW QUESTION 1
- (Exam Topic 1)
You are the security manager for a small application development company. Your company is considering the use of the cloud for software testing purposes. Which cloud service model is most likely to suit your needs?
Response:

A. IaaS
B. PaaS
C. SaaS
D. LaaS

Answer: B

NEW QUESTION 2
- (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 3
- (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 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)
The cloud deployment model that features organizational ownership of the hardware and infrastructure, and usage only by members of that organization, is known as:
Response:

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

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
Which of the following is a risk in the cloud environment that is not existing or is as prevalent in the legacy environment?
Response:

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

Answer: A

NEW QUESTION 7
- (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 8
- (Exam Topic 1)
Which of the following is a file server that provides data access to multiple, heterogeneous machines/users on the network?
Response:

A. Storage area network (SAN)
B. Network-attached storage (NAS)
C. Hardware security module (HSM)
D. Content delivery network (CDN)

Answer: B

NEW QUESTION 9
- (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)
You are in charge of creating the BCDR plan and procedures for your organization. Your organization has its production environment hosted by a cloud provider, and you have appropriate protections in place.
Which of the following is a significant consideration for your BCDR backup? Response:

A. Enough personnel at the BCDR recovery site to ensure proper operations
B. Good cryptographic key management
C. Access to the servers where the BCDR backup is stored
D. Forensic analysis capabilities

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
A typical DLP tool can enhance the organization’s efforts at accomplishing what legal task? Response:

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

Answer: A

NEW QUESTION 13
- (Exam Topic 1)
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 18
- (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 get truly holistic coverage of your environment, you should be sure to include _____ as a step in the deployment process.
Response:

A. Getting signed user agreements from all users
B. Installation of the solution on all assets in the cloud data center
C. Adoption of the tool in all routers between your users and the cloud provider

D. All of your customers to install the tool

Answer: A

NEW QUESTION 23
- (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 24
- (Exam Topic 1)
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
What should you not expect the tool to address? Response:

A. Sensitive data sent inadvertently in user emails
B. Sensitive data captured by screen shots
C. Sensitive data moved to external devices
D. Sensitive data in the contents of files sent via FTP

Answer: B

NEW QUESTION 26
- (Exam Topic 1)
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "cross-site scripting (XSS)."
Which of the following is not a method for reducing the risk of XSS attacks? Response:

A. Use an auto-escaping template system.
B. XML escape all identity assertions.
C. Sanitize HTML markup with a library designed for the purpose.
D. HTML escape JSON values in an HTML context and read the data with JSON.parse.

Answer: B

NEW QUESTION 28
- (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 31
- (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 34
- (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 35
- (Exam Topic 1)
Every cloud service provider that opts to join the CSA STAR program registry must complete a _____.

A. SOC 2, Type 2 audit report
B. Consensus Assessment Initiative Questionnaire (CAIQ)
C. NIST 800-37 RMF audit
D. ISO 27001 ISMS review

Answer: B

NEW QUESTION 39
- (Exam Topic 1)
What sort of legal enforcement may the Payment Card Industry (PCI) Security Standards Council not bring to bear against organizations that fail to comply with the Payment Card Industry Data Security Standard (PCI DSS)?
Response:

A. Fines
B. Jail time
C. Suspension of credit card processing privileges
D. Subject to increased audit frequency and scope

Answer: B

NEW QUESTION 42
- (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 47
- (Exam Topic 1)
TLS uses _____ to authenticate a connection and create a shared secret for the duration of the session.

A. SAML 2.0
B. X.509 certificates
C. 802.11X
D. The Diffie-Hellman process

Answer: B

NEW QUESTION 48
- (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 50
- (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 53
- (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 58
- (Exam Topic 1)
Which security certification serves as a general framework that can be applied to any type of system or application?

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

Answer: A

NEW QUESTION 63
- (Exam Topic 1)
One of the security challenges of operating in the cloud is that additional controls must be placed on file storage systems because _____ .
Response:

A. File stores are always kept in plain text in the cloud
B. There is no way to sanitize file storage space in the cloud
C. Virtualization necessarily prevents the use of application-based security controls
D. Virtual machines are stored as snapshotted files when not in use

Answer: D

NEW QUESTION 67
- (Exam Topic 1)
Which of the following are considered to be the building blocks of cloud computing? Response:

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

Answer: C

NEW QUESTION 71
- (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 72
- (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 77
- (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 81
- (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 84
- (Exam Topic 1)
What is the primary security mechanism used to protect SOAP and REST APIs? Response:

A. Firewalls
B. XML firewalls
C. Encryption
D. WAFs

Answer: C

NEW QUESTION 85
- (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 89
- (Exam Topic 1)
A honeypot should contain data_____.
Response:

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

Answer: C

NEW QUESTION 93
- (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 94
- (Exam Topic 1)
Impact resulting from risk being realized is often measured in terms of _____.

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

Answer: B

NEW QUESTION 96
- (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 99
- (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 101
- (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, all of the following activity can result in data loss except _____ .

A. Misplaced crypto keys
B. Improper policy
C. Ineffectual backup procedures
D. Accidental overwrite

Answer: B

NEW QUESTION 106
- (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 109
- (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 110
- (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 112
- (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 114
- (Exam Topic 2)

What is the intellectual property protection for the logo of a new video game? Response:

A. Copyright
B. Patent
C. Trademark
D. Trade secret

Answer: C

NEW QUESTION 117
- (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 120
- (Exam Topic 2)
Which SSAE 16 audit report is simply an attestation of audit results? Response:

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

Answer: D

NEW QUESTION 121
- (Exam Topic 2)
A process for _____ can aid in protecting against data disclosure due to lost devices. Response:

A. User punishment
B. Credential revocation
C. Law enforcement notification
D. Device tracking

Answer: B

NEW QUESTION 123
- (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 125
- (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 128
- (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 130
- (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 136
- (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 138
- (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 142
- (Exam Topic 2)
Which cloud service category is MOST likely to use a client-side key management system? Response:

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

Answer: B

NEW QUESTION 146
- (Exam Topic 2)
The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) addresses all the following security architecture elements except _____.
Response:

A. Physical security
B. IaaS
C. Application security
D. Business drivers

Answer: D

NEW QUESTION 150
- (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 152
- (Exam Topic 2)
Which of the following methods is often used to obscure data from production systems for use in test or development environments?
Response:

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

Answer: C

NEW QUESTION 156
- (Exam Topic 2)
Which of the following is not one of the types of controls? Response:

A. Transitional
B. Administrative
C. Technical
D. Physical

Answer: A

NEW QUESTION 161
- (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 166
- (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 167
- (Exam Topic 2)
Who should be involved in review and maintenance of user accounts/access? Response:

A. The user’s manager
B. The security manager
C. The accounting department
D. The incident response team

Answer: A

NEW QUESTION 172
- (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 174
- (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 179
- (Exam Topic 2)
You are the IT security manager for a video game software development company. Which of the following is most likely to be your primary concern on a daily basis?
Response:

A. Health and human safety
B. Security flaws in your products
C. Security flaws in your organization
D. Regulatory compliance

Answer: C

NEW QUESTION 184
- (Exam Topic 2)
You are a consultant performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost $24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant.
The fire suppression system costs $15 million. An insurance policy that would cover the full replacement cost of the plant costs $1 million per month.
In order to establish the true annualized loss expectancy (ALE), you would need all of the following information except _____ .
Response:

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

Answer: D

NEW QUESTION 189
- (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 192
- (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 194
- (Exam Topic 2)
Resolving resource contentions in the cloud will most likely be the job of the _____.
Response:

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

Answer: D

NEW QUESTION 199
- (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 202
- (Exam Topic 2)
Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider? Response:

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

Answer: D

NEW QUESTION 206
- (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 209
- (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 210
- (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 213
- (Exam Topic 2)
Tokenization requires at least _____ database(s).
Response:

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

Answer: B

NEW QUESTION 214
- (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 219
- (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 221
- (Exam Topic 2)
All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline, except _____.
Response:

A. Audit the baseline to ensure that all configuration items have been included and applied correctly
B. Impose the baseline throughout the environment
C. Capture an image of the baseline system for future reference/versioning/rollback purposes
D. Document all baseline configuration elements and versioning data

Answer: B

NEW QUESTION 225
- (Exam Topic 2)
Which of the following is not a feature of SAST? Response:

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

Answer: B

NEW QUESTION 229
- (Exam Topic 2)
Your organization is considering a move to a cloud environment and is looking for certifications or audit reports from cloud providers to ensure adequate security controls and processes.
Which of the following is NOT a security certification or audit report that would be pertinent? Response:

A. FedRAMP
B. PCI DSS
C. FIPS 140-2
D. SOC Type 2

Answer: C

NEW QUESTION 231
- (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 236
- (Exam Topic 2)
Halon is now illegal to use for data center fire suppression. What is the reason it was outlawed? Response:

A. It poses a threat to health and human safety when deployed.
B. It can harm the environment.
C. It does not adequately suppress fires.
D. It causes undue damage to electronic systems.

Answer: B

NEW QUESTION 237
- (Exam Topic 2)
What is a form of cloud storage where data is stored as objects, arranged in a hierarchal structure, like a file tree?

Response:

A. Volume storage
B. Databases
C. Content delivery network (CDN)
D. Object storage

Answer: D

NEW QUESTION 242
- (Exam Topic 2)
All of the following are identity federation standards commonly found in use today except _____.
Response:

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

Answer: D

NEW QUESTION 245
- (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 248
- (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 252
- (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 255
- (Exam Topic 2)
All of the following might be used as data discovery characteristics in a content-analysis-based data discovery effort except _____.
Response:

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

Answer: D

NEW QUESTION 256
- (Exam Topic 2)
Federation should be _____ to the users.
Response:

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

Answer: C

NEW QUESTION 259
- (Exam Topic 2)
The Restatement (Second) Conflict of Law refers to which of the following? Response:

A. The basis for deciding which laws are most appropriate in a situation where conflicting laws exist
B. When judges restate the law in an opinion
C. How jurisdictional disputes are settled
D. Whether local or federal laws apply in a situation

Answer: A

NEW QUESTION 260
- (Exam Topic 2)
What is a cloud storage architecture that manages the data in caches of copied content close to locations of high demand?
Response:

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

Answer: D

NEW QUESTION 265
- (Exam Topic 2)
_____ can often be the result of inadvertent activity. Response:

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

Answer: C

NEW QUESTION 269
- (Exam Topic 2)
Your organization is developing software for wide use by the public. You have decided to test it in a cloud environment, in a PaaS model. Which of the following should be of particular concern to your organization for this situation?
Response:

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

Answer: B

NEW QUESTION 273
- (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 278
- (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 279
- (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 284
- (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 288
- (Exam Topic 3)
You work for a company that operates a production environment in the cloud. Another company using the same cloud provider is under investigation by law enforcement for racketeering.
Your company should be concerned about this because of the cloud characteristic of . Response:

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

Answer: B

NEW QUESTION 291
- (Exam Topic 3)
A user signs on to a cloud-based social media platform. In another browser tab, the user finds an article worth posting to the social media platform. The user clicks on the platform's icon listed on the article's website, and the article is automatically posted to the user's account on the social media platform.
This is an example of what?
Response:

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

Answer: C

NEW QUESTION 295
- (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 300
- (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 305
- (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 306
- (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 307
- (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 309
- (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 311
- (Exam Topic 3)
What is the main reason virtualization is used in the cloud? Response:

A. VMs are easier to administer
B. If a VM is infected with malware, it can be easily replaced
C. With VMs, the cloud provider does not have to deploy an entire hardware device for every new user
D. VMs are easier to operate than actual devices

Answer: C

NEW QUESTION 315
- (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 317
- (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 318
- (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 319
- (Exam Topic 3)
Which type of cloud-based storage is IRM typically associated with? Response:

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

Answer: D

NEW QUESTION 322
- (Exam Topic 3)
Which of the following data-sanitation approaches are always available within a cloud environment? Response:

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

Answer: D

NEW QUESTION 325
- (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 326
- (Exam Topic 3)
Cloud environments are based entirely on virtual machines and virtual devices, and those images are also in need of storage within the environment. What type of storage is typically used for virtual images?
Response:

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

Answer: D

NEW QUESTION 330
- (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 333
- (Exam Topic 3)
Which of the following aids in the ability to demonstrate due diligence efforts?
Response:

A. Redundant power lines

B. HVAC placement
C. Security training documentation
D. Bollards

Answer: C

NEW QUESTION 337
- (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 338
- (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 341
- (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 343
- (Exam Topic 3)
With data in transit, which of the following will be the MOST major concern in order for a DLP solution to properly work?
Response:

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

Answer: B

NEW QUESTION 344
- (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 347
- (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)
Which of the following is not included in the OWASP Top Ten web application security threats? Response:

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

Answer: C

NEW QUESTION 356
- (Exam Topic 3)
What type of identity system allows trust and verifications between the authentication systems of multiple organizations?
Response:

A. Federated
B. Collaborative
C. Integrated
D. Bidirectional

Answer: A

NEW QUESTION 361
- (Exam Topic 3)
When a user accesses a system, what process determines the roles and privileges that user is granted within the application?
Response:

A. Authorization
B. Authentication
C. Provisioning
D. Privilege

Answer: A

NEW QUESTION 364
- (Exam Topic 3)
It’s important to maintain a current asset inventory list, including surveying your environment on a regular basis, in order to _____ .
Response:

A. Prevent unknown, unpatched assets from being used as back doors to the environment
B. Ensure that any lost devices are automatically entered into the acquisition system for repurchasing and replacement
C. Maintain user morale by having their devices properly catalogued and annotated
D. Ensure that billing for all devices is handled by the appropriate departments

Answer: A

NEW QUESTION 365
- (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 366
- (Exam Topic 3)
Tokenization requires two distinct _____.

Response:

A. Authentication factors
B. Databases
C. Encryption keys
D. Personnel

Answer: B

NEW QUESTION 370
- (Exam Topic 3)
An audit against the _____ will demonstrate that an organization has a holistic, comprehensive security program.
Response:

A. SAS 70 standard
B. SSAE 16 standard
C. SOC 2, Type 2 report matrix
D. ISO 27001 certification requirements

Answer: D

NEW QUESTION 375
- (Exam Topic 3)
Which of the following is not a security concern related to archiving data for long-term storage? Response:

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

Answer: D

NEW QUESTION 378
- (Exam Topic 3)
Which of the following types of software is a Type 2 hypervisor dependent on that a Type 1 hypervisor isn't? Response:

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

Answer: C

NEW QUESTION 382
- (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 385
- (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 387
- (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 388
- (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 390
- (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 392
- (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 394
- (Exam Topic 3)
_____ is perhaps the main external factor driving IAM efforts. Response:

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

Answer: A

NEW QUESTION 398
- (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 401
- (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 403
- (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 404
- (Exam Topic 3)
Bob is staging an attack against Alice's website. He is able to embed a link on her site that will execute malicious code on a visitor's machine, if the visitor clicks on the link. This is an example of which type of attack?
Response:

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

Answer: A

NEW QUESTION 407
.....

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