ISC2

Exam Questions CCSP

Certified Cloud Security Professional

NEW QUESTION 1
- (Exam Topic 1)
A virtual network interface card (NIC) exists at layer _____ of the OSI model. Response:

A. 2
B. 4
C. 6
D. 8

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
Under EU law, a cloud customer who gives sensitive data to a cloud provider is still legally responsible for the damages resulting from a data breach caused by the provider; the EU would say that it is the cloud customer's fault for choosing the wrong provider.
This is an example of insufficient _____ .

A. Proof
B. Evidence
C. Due diligence
D. Application of reasonableness

Answer: C

NEW QUESTION 3
- (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 4
- (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 5
- (Exam Topic 1)
According to the (ISC)2 Cloud Secure Data Life Cycle, which phase comes soon after (or at the same time as) the Create phase?

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

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
What is used with a single sign-on system for authentication after the identity provider has successfully authenticated a user?
Response:

A. Token
B. Key
C. XML
D. SAML

Answer: A

NEW QUESTION 7
- (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 8
- (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 9
- (Exam Topic 1)
You have been tasked with creating an audit scope statement and are making your project outline. Which of the following is NOT typically included in an audit scope statement?

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

Answer: D

NEW QUESTION 10
- (Exam Topic 1)
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 10
- (Exam Topic 1)
Which phase of the cloud data lifecycle involves processing by a user or application? Response:

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

Answer: D

NEW QUESTION 14
- (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 18
- (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 21
- (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 25
- (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 30
- (Exam Topic 1)
_____ is the legal concept whereby a cloud customer is held to a reasonable expectation for providing security of its users' and clients' privacy data in their control.
Response:

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

Answer: B

NEW QUESTION 33
- (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 34
- (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 36
- (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 41

- (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 43
- (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 47
- (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 52
- (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 53
- (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 55
- (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 57
- (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)
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 63
- (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 64
- (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 69
- (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 70
- (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 74
- (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 78
- (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 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 86
- (Exam Topic 1)
Data labels could include all the following, except: Response:

A. Source
B. Delivery vendor
C. Handling restrictions
D. Jurisdiction

Answer: B

NEW QUESTION 88
- (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 89
- (Exam Topic 1)
When an organization considers cloud migrations, the organization's software developers will need to know which _____ and _____ which the organization will be using, in order to properly and securely create suitable applications.

A. Geographic location, native language
B. Legal restrictions, specific ISP
C. Service model, deployment model
D. Available bandwidth, telecommunications country code

Answer: C

NEW QUESTION 94
- (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 97
- (Exam Topic 1)
During which stage of the SDLC process should security be consulted and begin its initial involvement?

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

Answer: D

NEW QUESTION 102
- (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)
Which cloud service category offers the most customization options and control to the cloud customer?
Response:

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

Answer: B

NEW QUESTION 110
- (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 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)
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 120
- (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 125
- (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 127
- (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 130
- (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 133
- (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 134
- (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 138
- (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 139
- (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 142
- (Exam Topic 2)
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
Which of these activities should you perform before deploying the tool? Response:

A. Survey your company's departments about the data under their control
B. Reconstruct your firewalls
C. Harden all your routers
D. Adjust the hypervisors

Answer: A

NEW QUESTION 146
- (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 148
- (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 153
- (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 155
- (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 156
- (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 161
- (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 164
- (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 169
- (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 172
- (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 177
- (Exam Topic 2)
Which one of the following is not one of the three common threat modeling techniques? Response:

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

Answer: D

NEW QUESTION 180
- (Exam Topic 2)
Although encryption can help an organization to effectively decrease the possibility of data breaches, which other type of threat can it increase the chances of?
Response:

A. Insecure interfaces
B. Data loss

C. System vulnerabilities
D. Account hijacking

Answer: B

NEW QUESTION 185
- (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 190
- (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 194
- (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 197
- (Exam Topic 2)
What is the risk to the organization posed by dashboards that display data discovery results? Response:

A. Increased chance of external penetration
B. Flawed management decisions based on massaged displays
C. Higher likelihood of inadvertent disclosure
D. Raised incidence of physical theft

Answer: B

NEW QUESTION 199
- (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 203
- (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 204
- (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 206
- (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 209
- (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 211
- (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 212
- (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 213
- (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 214

- (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 217
- (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 220
- (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 224
- (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 229
- (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 232
- (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 237
- (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 241
- (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 245
- (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 247
- (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 252
- (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 256
- (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 261
- (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 264
- (Exam Topic 2)
Which type of testing tends to produce the best and most comprehensive results for discovering system vulnerabilities?
Response:

A. Static
B. Dynamic
C. Pen
D. Vulnerability

Answer: A

NEW QUESTION 269
- (Exam Topic 2)
All of the following methods can be used to attenuate the harm caused by escalation of privilege except: Response:

A. Extensive access control and authentication tools and techniques
B. Analysis and review of all log data by trained, skilled personnel on a frequent basis
C. Periodic and effective use of cryptographic sanitization tools
D. The use of automated analysis tools such as SIM, SIEM, and SEM solutions

Answer: C

NEW QUESTION 273
- (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 276
- (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 278
- (Exam Topic 2)
DLP solutions typically involve all of the following aspects except _____.
Response:

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

Answer: B

NEW QUESTION 279
- (Exam Topic 2)
_____ can often be the result of inadvertent activity. Response:

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

Answer: C

NEW QUESTION 280
- (Exam Topic 2)
When considering the option to migrate from an on-premises environment to a hosted cloud service, an organization should weigh the risks of allowing external entities to access the cloud data for collaborative purposes against _____.
Response:

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

Answer: D

NEW QUESTION 284
- (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 288
- (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 292
- (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 294
- (Exam Topic 3)
Which of the following is NOT one of the security domains presented within the Cloud Controls Matrix? Response:

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

Answer: A

NEW QUESTION 295
- (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 298
- (Exam Topic 3)
Cloud vendors are held to contractual obligations with specified metrics by:
Response:

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

Answer: A

NEW QUESTION 302
- (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 307
- (Exam Topic 3)
Which technology is most associated with tunneling? Response:

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

Answer: B

NEW QUESTION 310
- (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 314
- (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 318
- (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 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 321
- (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 324
- (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 325
- (Exam Topic 3)
Typically, SSDs are _____.
Response:

A. More expensive than spinning platters
B. Larger than tape backup
C. Heavier than tape libraries
D. More subject to malware than legacy drives

Answer: A

NEW QUESTION 327
- (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 329
- (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 333
- (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 335
- (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 337
- (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 341
- (Exam Topic 3)
You are developing a new process for data discovery for your organization and are charged with ensuring that all applicable data is included. Which of the following is NOT one of the three methods of data discovery?
Response:

A. Metadata
B. Content analysis
C. Labels
D. Classification

Answer: D

NEW QUESTION 343
- (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 344
- (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 349
- (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 350
- (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 352
- (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 355
- (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 359
- (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 360
- (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 363
- (Exam Topic 3)
You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally.
Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes. Your company has decided to expand its business to include selling and monitoring life-support equipment for medical providers.
What characteristic do you need to ensure is offered by your cloud provider? Response:

A. Full automation of security controls within the cloud data center
B. Tier 4 of the Uptime Institute certifications
C. Global remote access
D. Prevention of ransomware infections

Answer: B

NEW QUESTION 367
- (Exam Topic 3)
What is the major difference between authentication/authorization? Response:

A. Code verification/code implementation
B. Identity validation/access permission
C. Inverse incantation/obverse instantiation
D. User access/privileged access

Answer: B

NEW QUESTION 369
- (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 370
- (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 372
- (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 375
- (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 377
- (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 378
- (Exam Topic 3)
Anonymization is the process of removing from data sets. Response:

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

Answer: D

NEW QUESTION 380
- (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 381
- (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 386
- (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 390
- (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 392
- (Exam Topic 3)
What are the objectives of change management? (Choose all that apply.)
Response:

A. Respond to a customer’s changing business requirements while maximizing value and reducing incidents, disruption, and rework
B. Ensure that changes are recorded and evaluated
C. Respond to business and IT requests for change that will disassociate services with business needs
D. Ensure that all changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner

Answer: AB

NEW QUESTION 394
- (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 399
- (Exam Topic 3)
Which of the following is a risk that stems from a virtualized environment? Response:

A. Live virtual machines in the production environment are moved from one host to another in the clear.
B. Cloud data centers can become a single point of failure.
C. It is difficult to find and contract with multiple utility providers of the same type (electric, water, etc.).
D. Modern SLA demands are stringent and very hard to meet.

Answer: A

NEW QUESTION 402
- (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 406
- (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 410
- (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 413
- (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 416
- (Exam Topic 3)
Alice is the CEO for a software company; she is considering migrating the operation from the current on-premises legacy environment into the cloud.
In order to protect her company's intellectual property, Alice might want to consider implementing all these techniques/solutions except _____.
Response:

A. Egress monitoring
B. Encryption
C. Turnstiles
D. Digital watermarking

Answer: C

NEW QUESTION 419
- (Exam Topic 3)
Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?
Response:

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

Answer: B

NEW QUESTION 423
- (Exam Topic 3)
You work for a government research facility. Your organization often shares data with other government research organizations.
You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations.
Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.

In order to pass the user IDs and authenticating credentials of each user among the organizations, what protocol/language/motif will you most likely utilize? Response:

A. Representational State Transfer (REST)
B. Security Assertion Markup Language (SAML)
C. Simple Object Access Protocol (SOAP)
D. Hypertext Markup Language (HTML)

Answer: B

NEW QUESTION 426
- (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 431
- (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 432
- (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 434
- (Exam Topic 3)
In general, a cloud BCDR solution will be _____ than a physical solution. Response:

A. Slower
B. Less expensive
C. Larger
D. More difficult to engineer

Answer: B

NEW QUESTION 436
- (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 438
- (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 440
- (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 443
.....

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