Exam Questions CCSP

Certified Cloud Security Professional

https://www.2passeasy.com/dumps/CCSP/

NEW QUESTION 1
- (Exam Topic 1)
Vulnerability scans are dependent on _____ in order to function. Response:

A. Privileged access
B. Vulnerability signatures
C. Malware libraries
D. Forensic analysis

Answer: B

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

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

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
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 4
- (Exam Topic 1)
Which strategy involves using a fake production system to lure attackers in order to learn about their tactics?
Response:

A. IDS
B. Honeypot
C. IPS
D. Firewall

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
All of the following are usually nonfunctional requirements except _____.
Response:

A. Color
B. Sound
C. Security
D. Function

Answer: D

NEW QUESTION 6
- (Exam Topic 1)
Which of the following is characterized by a set maximum capacity? Response:

A. A secret-sharing-made-short (SSMS) bit-splitting implementation
B. A tightly coupled cloud storage cluster
C. A loosely coupled cloud storage cluster
D. A public-key infrastructure

Answer: B

NEW QUESTION 7
- (Exam Topic 1)
What type of device is often leveraged to assist legacy applications that may not have the programmatic capability to process assertions from modern web services?

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

Answer: B

NEW QUESTION 8
- (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 9
- (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 10
- (Exam Topic 1)
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “unvalidated redirects and forwards.”
Which of the following is a good way to protect against this problem? Response:

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

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
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 12
- (Exam Topic 1)
Which of the following best describes SAML? Response:

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

Answer: B

NEW QUESTION 15
- (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 17
- (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 22
- (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 24
- (Exam Topic 1)
The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet). In a typical TLS session, who initiates the protocol?
Response:

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

Answer: B

NEW QUESTION 28
- (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 33
- (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 34
- (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 37
- (Exam Topic 1)
Which of the following tools might be useful in data discovery efforts that are based on content analysis?

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

Answer: A

NEW QUESTION 40
- (Exam Topic 1)
You are performing an audit of the security controls used in a cloud environment. Which of the following would best serve your purpose?
Response:

A. The business impact analysis (BIA)
B. A copy of the VM baseline configuration
C. The latest version of the company's financial records
D. A SOC 3 report from another (external) auditor

Answer: B

NEW QUESTION 44
- (Exam Topic 1)
Which of the following is a method for apportioning resources that involves setting guaranteed minimums for all tenants/customers within the environment?
Response:

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

Answer: A

NEW QUESTION 46
- (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 49
- (Exam Topic 1)
Which of the following storage types are used with an Infrastructure as a Service (IaaS) solution? Response:

A. Volume and block
B. Structured and object
C. Unstructured and ephemeral
D. Volume and object

Answer: D

NEW QUESTION 53
- (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 55
- (Exam Topic 1)
Which of the following is the recommended operating range for temperature and humidity in a data center?
Response:

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

C. Between 64 °F - 84 °F and 30% and 60% relative humidity
D. Between 60 °F - 85 °F and 40% and 60% relative humidity

Answer: B

NEW QUESTION 60
- (Exam Topic 1)
Which of the following practices can enhance both operational capabilities and configuration management efforts?
Response:

A. Regular backups
B. Constant uptime
C. Multifactor authentication
D. File hashes

Answer: D

NEW QUESTION 64
- (Exam Topic 1)
Which of the following is a possible negative aspect of bit-splitting?

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

Answer: C

NEW QUESTION 66
- (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 68
- (Exam Topic 1)
You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider.
Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also allow users to select which APIs they install and use on their own devices in order to access and manipulate company data.
Of the following, what is a security control you'd like to implement to offset the risk(s) incurred by this practice?

A. Regular and widespread integrity checks on sampled data throughout the managed environment
B. More extensive and granular background checks on all employees, particularly new hires
C. Inclusion of references to all applicable regulations in the policy documents
D. Increased enforcement of separation of duties for all workflows

Answer: A

NEW QUESTION 70
- (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 74
- (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 79
- (Exam Topic 1)
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing?
Response:

A. Most of the cloud customer's interaction with resources will be performed through APIs.
B. APIs are inherently insecure.
C. Attackers have already published vulnerabilities for all known APIs.
D. APIs are known carcinogens.

Answer: A

NEW QUESTION 82
- (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 87
- (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)
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 90
- (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 95
- (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 99
- (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 104
- (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 105
- (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 107
- (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 110
- (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 113
- (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 114

- (Exam Topic 1)
Data labels could include all the following, except: Response:

A. Confidentiality level
B. Distribution limitations
C. Access restrictions
D. Multifactor authentication

Answer: D

NEW QUESTION 119
- (Exam Topic 1)
_____ is the most prevalent protocol used in identity federation.

A. HTTP
B. SAML
C. FTP
D. WS-Federation

Answer: B

NEW QUESTION 124
- (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 128
- (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 130
- (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 134
- (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 136
- (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 139
- (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 142
- (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 144
- (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 149
- (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 151
- (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 155
- (Exam Topic 2)
The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program has _____ tiers. Response:

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

Answer: B

NEW QUESTION 159

- (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 164
- (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 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 170
- (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 172
- (Exam Topic 2)
Which of the following is a method for apportioning resources that involves setting maximum usage amounts for all tenants/customers within the environment? Response:

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

Answer: D

NEW QUESTION 173
- (Exam Topic 2)
All of the following entitles are required to use FedRAMP-accredited Cloud Service Providers except _____.
Response:

A. The US post office
B. The Department of Homeland Security
C. Federal Express
D. The CIA

Answer: C

NEW QUESTION 176
- (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 180
- (Exam Topic 2)
Although performing BCDR tests at regular intervals is a best practice to ensure processes and documentation are still relevant and efficient, which of the following represents a reason to conduct a BCDR review outside of the regular interval?
Response:

A. Staff changes
B. Application changes
C. Regulatory changes
D. Management changes

Answer: B

NEW QUESTION 182
- (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 185
- (Exam Topic 2)
Which of the following would probably best aid an organization in deciding whether to migrate from a legacy environment to a particular cloud provider?
Response:

A. Rate sheets comparing a cloud provider to other cloud providers
B. Cloud provider offers to provide engineering assistance during the migration
C. The cost/benefit measure of closing the organization’s relocation site (hot site/warm site) and using the cloud for disaster recovery instead
D. SLA satisfaction surveys from other (current and past) cloud customers

Answer: D

NEW QUESTION 186
- (Exam Topic 2) 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 189
- (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 192
- (Exam Topic 2)
Before deploying a specific brand of virtualization toolset, it is important to configure it according to
_____ .
Response:

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

Answer: C

NEW QUESTION 195
- (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 199
- (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 203
- (Exam Topic 2)
You are the security manager for a company that is considering cloud migration to an IaaS environment. You are assisting your company's IT architects in constructing the environment. Which of the following options do you recommend?
Response:

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

Answer: B

NEW QUESTION 207
- (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 210
- (Exam Topic 2)
There are two general types of smoke detectors. Which type uses a small portion of radioactive material? Response:

A. Photoelectric
B. Ionization
C. Electron pulse
D. Integral field

Answer: B

NEW QUESTION 213
- (Exam Topic 2)
Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?
Response:

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

Answer: C

NEW QUESTION 215
- (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 217
- (Exam Topic 2)
What are the four cloud deployment models? Response:

A. Public, Internal, Hybrid, and Community
B. External, Private, Hybrid, and Community
C. Public, Private, Joint, and Community
D. Public, Private, Hybrid, and Community

Answer: D

NEW QUESTION 218
- (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 220
- (Exam Topic 2)
Which of the following contract terms most incentivizes the cloud provider to meet the requirements listed in the SLA?
Response:

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

Answer: B

NEW QUESTION 225
- (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 228
- (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 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 235
- (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 principle must always been included with an SOC 2 report? Response:

A. Confidentiality
B. Security
C. Privacy
D. Processing integrity

Answer: B

NEW QUESTION 238
- (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 243
- (Exam Topic 2)
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 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 250
- (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 251
- (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 253
- (Exam Topic 2)
TLS provides _____ and _____ for communications. Response:

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

Answer: C

NEW QUESTION 257
- (Exam Topic 2)
Which phase of the cloud data lifecycle also typically entails the process of data classification? Response:

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

Answer: C

NEW QUESTION 261
- (Exam Topic 2) What is a key component of GLBA? Response:

A. The right to be forgotten
B. EU Data Directives
C. The information security program
D. The right to audit

Answer: C

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

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

Answer: B

NEW QUESTION 270
- (Exam Topic 2)
Federation should be _____ to the users.
Response:

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

Answer: C

NEW QUESTION 272
- (Exam Topic 2)
Which of the following in a federated environment is responsible for consuming authentication tokens? Response:

A. Relying party
B. Identity provider
C. Cloud services broker
D. Authentication provider

Answer: A

NEW QUESTION 273
- (Exam Topic 2)
Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company's website)?
Response:

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

Answer: D

NEW QUESTION 276
- (Exam Topic 2)
Which type of report is considered for "general" use and does not contain any sensitive information? Response:

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

Answer: C

NEW QUESTION 279
- (Exam Topic 2)
What is a data custodian responsible for? Response:

A. The safe custody, transport, storage of the data, and implementation of business rules
B. Data content, context, and associated business rules
C. Logging and alerts for all data
D. Customer access and alerts for all data

Answer: A

NEW QUESTION 282
- (Exam Topic 2)
You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization.
What is probably the best benefit offered by the CCM? Response:

A. The low cost of the tool
B. Allowing your organization to leverage existing controls across multiple frameworks so as not to duplicate effort
C. Simplicity of control selection from the list of approved choices
D. Ease of implementation by choosing controls from the list of qualified vendors

Answer: B

NEW QUESTION 286
- (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 289
- (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 292
- (Exam Topic 2)
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 296
- (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 297
- (Exam Topic 2)
Which of the following is NOT a common component of a DLP implementation process? Response:

A. Discovery
B. Monitoring
C. Revision
D. Enforcement

Answer: C

NEW QUESTION 301
- (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 303
- (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 306
- (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 310
- (Exam Topic 3)
Which technology is most associated with tunneling? Response:

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

Answer: B

NEW QUESTION 315
- (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 320
- (Exam Topic 3)
During the assessment phase of a risk evaluation, what are the two types of tests that are performed? Response:

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

Answer: D

NEW QUESTION 323
- (Exam Topic 3)
Which of the following threats from the OWASP Top Ten is the most difficult for an organization to protect against?
Response:

A. Advanced persistent threats
B. Account hijacking
C. Malicious insiders
D. Denial of service

Answer: C

NEW QUESTION 326
- (Exam Topic 3)
Fiber-optic lines are considered part of layer _____ of the OSI model. Response:

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

Answer: A

NEW QUESTION 330
- (Exam Topic 3)
Which of the following is not a component of the of the STRIDE model? Response:

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

Answer: D

NEW QUESTION 335
- (Exam Topic 3)

The ISO/IEC 27001:2013 security standard contains 14 different domains that cover virtually all areas of IT operations and procedures. Which of the following is NOT one of the domains listed in the standard?
Response:

A. Legal
B. Management
C. Assets
D. Supplier Relationships

Answer: A

NEW QUESTION 338
- (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 340
- (Exam Topic 3)
A loosely coupled storage cluster will have performance and capacity limitations based on the _____.
Response:

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

Answer: D

NEW QUESTION 343
- (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 347
- (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 352
- (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 354
- (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 355
- (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 359
- (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 361
- (Exam Topic 3)
Your company maintains an on-premises data center for daily production activities but wants to use a cloud service to augment this capability during times of increased demand (cloud bursting).
Which deployment model would probably best suit the company’s needs? Response:

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

Answer: D

NEW QUESTION 364
- (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 366
- (Exam Topic 3)
All of these are reasons an organization may want to consider cloud migration except: Response:

A. Reduced personnel costs
B. Elimination of risks
C. Reduced operational expenses
D. Increased efficiency

Answer: B

NEW QUESTION 368
- (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 370
- (Exam Topic 3)
What aspect of a Type 2 hypervisor involves additional security concerns that are not relevant with a Type 1 hypervisor?
Response:

A. Reliance on a host operating system
B. Auditing
C. Proprietary software
D. Programming languages

Answer: A

NEW QUESTION 373
- (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 378
- (Exam Topic 3)
Which type of web application monitoring most closely measures actual activity? Response:

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

Answer: B

NEW QUESTION 383
- (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 386
- (Exam Topic 3)
Tokenization requires two distinct _____.
Response:

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

Answer: B

NEW QUESTION 390
- (Exam Topic 3)
Your company operates in a highly competitive market, with extremely high-value data assets. Senior management wants to migrate to a cloud environment but is concerned that providers will not meet the company's security needs.
Which deployment model would probably best suit the company's needs? Response:

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

Answer: B

NEW QUESTION 391
- (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 392
- (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 397
- (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 399
- (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 403
- (Exam Topic 3) Who operates the management plane? Response:

A. Regulators
B. End consumers
C. Privileged users
D. Privacy data subjects

Answer: C

NEW QUESTION 408
- (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 412
- (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 415

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

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

Answer: D

NEW QUESTION 420
- (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 421
- (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 425
- (Exam Topic 3)
Your application has been a continued target for SQL injection attempts. Which of the following technologies would be best used to combat the likeliness of a successful SQL injection exploit from occurring?
Response:

A. XML accelerator
B. WAF
C. Sandbox
D. Firewall

Answer: B

NEW QUESTION 429
- (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 433
- (Exam Topic 3)
Software-defined networking (SDN) is intended to separate different network capabilities and allow for the granting of granular configurations, permissions, and features to non-network staff or customers. Which network capability is separated from forwarding of traffic?
Response:

A. Routing
B. Firewalling
C. Filtering
D. IPS

Answer: C

NEW QUESTION 434
- (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 436
- (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 440
- (Exam Topic 3)
Setting thermostat controls by measuring the temperature will result in the _____ highest energy costs. Response:

A. Server inlet
B. Return air
C. Under-floor
D. External ambient

Answer: B

NEW QUESTION 444
- (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 448
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CCSP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CCSP Product From:

https://www.2passeasy.com/dumps/CCSP/

Money Back Guarantee

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