CCSP Dumps

Certified Cloud Security Professional

https://www.certleader.com/CCSP-dumps.html
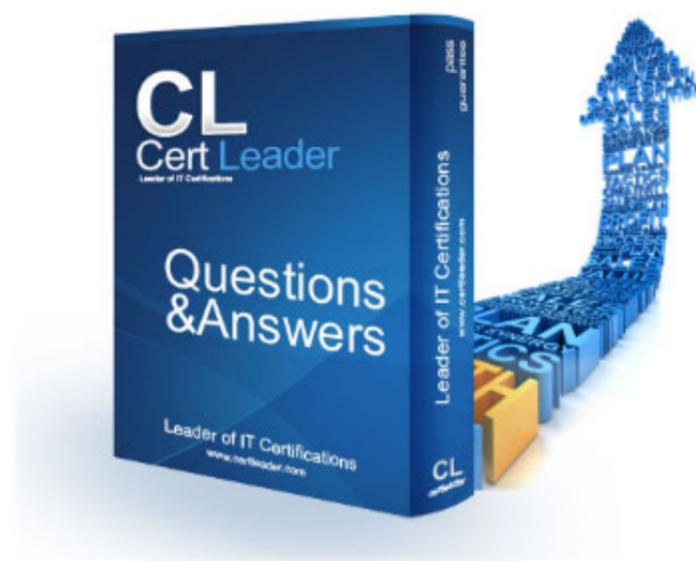
NEW QUESTION 1
- (Exam Topic 1)
Vulnerability scans are dependent on _____ in order to function. Response:

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

Answer: B

NEW QUESTION 2
- (Exam Topic 1)
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 3
- (Exam Topic 1)
_____ can often be the result of inadvertent activity. Response:

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

Answer: C

NEW QUESTION 4
- (Exam Topic 1) What can tokenization be used for? Response:

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

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
DLP can be combined with what other security technology to enhance data controls? Response:

A. DRM
B. SIEM
C. Kerberos
D. Hypervisors

Answer: A

NEW QUESTION 6
- (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 7
- (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 8
- (Exam Topic 1)
Which cloud storage type uses an opaque value or descriptor to categorize and organize data? Response:

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

Answer: D

NEW QUESTION 9
- (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 10
- (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)
Which of the following is a risk in the cloud environment that is not existing or is as prevalent in the legacy environment?
Response:

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

Answer: A

NEW QUESTION 12
- (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 15
- (Exam Topic 1)
What is the federal agency that accepts applications for new patents?

A. USDA
B. USPTO
C. OSHA
D. SEC

Answer: B

NEW QUESTION 18
- (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 19
- (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 24
- (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 28
- (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 30
- (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 35
- (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 37
- (Exam Topic 1)
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
In order to get truly holistic coverage of your environment, you should be sure to include _____ as a step in the deployment process.
Response:

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

D. All of your customers to install the tool

Answer: A

NEW QUESTION 40
- (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 45
- (Exam Topic 1)
At which phase of the SDLC process should security begin participating?

A. Requirements gathering
B. Requirements analysis
C. Design
D. Testing

Answer: A

NEW QUESTION 47
- (Exam Topic 1)
Which of the following is the best and only completely secure method of data destruction? Response:

A. Degaussing
B. Crypto-shredding
C. Physical destruction of resources that store the data
D. Legal order issued by the prevailing jurisdiction where the data is geographically situated

Answer: C

NEW QUESTION 50
- (Exam Topic 1)
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 54
- (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 58
- (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 59
- (Exam Topic 1)
The cloud deployment model that features joint ownership of assets among an affinity group is known as: Response:

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

Answer: D

NEW QUESTION 61
- (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 65
- (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 68
- (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 71
- (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 74
- (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 76
- (Exam Topic 1)
TLS uses _____ to authenticate a connection and create a shared secret for the duration of the session.

A. SAML 2.0
B. X.509 certificates

C. 802.11X
D. The Diffie-Hellman process

Answer: B

NEW QUESTION 78
- (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 82
- (Exam Topic 1)
Which of the following is the correct name for Tier II of the Uptime Institute Data Center Site Infrastructure Tier Standard Topology?

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

Answer: D

NEW QUESTION 85
- (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 86
- (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 91
- (Exam Topic 1)
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:
Response:

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

Answer: B

NEW QUESTION 95
- (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 97
- (Exam Topic 1)
Using one cloud provider for your operational environment and another for your BCDR backup will also give you the additional benefit of _____.
Response:

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

Answer: B

NEW QUESTION 98
- (Exam Topic 1)
Which concept pertains to cloud customers paying only for the resources they use and consume, and only for the duration they are using them?
Response:

A. Measured service
B. Auto-scaling
C. Portability
D. Elasticity

Answer: A

NEW QUESTION 102
- (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 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, an organization that suffers a data breach might suffer all of the following negative effects except _____.
Response:

A. Cost of compliance with notification laws
B. Loss of public perception/goodwill
C. Loss of market share
D. Cost of detection

Answer: D

NEW QUESTION 108
- (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 113
- (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 116
- (Exam Topic 1)
What is the amount of fuel that should be on hand to power generators for backup datacenter power, in all tiers, according to the Uptime Institute?

A. 1
B. 1,000 gallons
C. 12 hours

D. As much as needed to ensure all systems may be gracefully shut down and data securely stored

Answer: C

NEW QUESTION 117
- (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 120
- (Exam Topic 1)
DRM solutions should generally include all the following functions, except:

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

Answer: B

NEW QUESTION 121
- (Exam Topic 1)
You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Previous releases have shipped with major flaws that were not detected in the testing phase; leadership wants to avoid repeating that problem. What tool/technique/technology might you suggest to aid in identifying programming errors?

A. Vulnerability scans
B. Open source review
C. SOC audits
D. Regulatory review

Answer: B

NEW QUESTION 125
- (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 128
- (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 130
- (Exam Topic 1)
A honeypot should contain data_____.
Response:

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

Answer: C

NEW QUESTION 132

- (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 134
- (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 138
- (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 140
- (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 141
- (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 145
- (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 148
- (Exam Topic 1)
The use of which of the following technologies will NOT require the security dependency of an operating system, other than its own?

A. Management plane
B. Type 1 hypervisor
C. Type 2 hypervisor
D. Virtual machine

Answer: B

NEW QUESTION 151
- (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 152
- (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 156
- (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 161
- (Exam Topic 2)
Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?
Response:

A. Mapping to existing access control lists (ACLs)
B. Delineating biometric catalogs
C. Preventing multifactor authentication
D. Prohibiting unauthorized transposition

Answer: A

NEW QUESTION 165
- (Exam Topic 2)
Which SSAE 16 audit report is simply an attestation of audit results? Response:

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

Answer: D

NEW QUESTION 168
- (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 173
- (Exam Topic 2)

A bare-metal hypervisor is Type _____.
Response:

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

Answer: A

NEW QUESTION 176
- (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 179
- (Exam Topic 2)
The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) addresses all the following security architecture elements except _____.
Response:

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

Answer: D

NEW QUESTION 182
- (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 184
- (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 189
- (Exam Topic 2)
Which of the following is not one of the types of controls? Response:

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

Answer: A

NEW QUESTION 192
- (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 195
- (Exam Topic 2)
You are the IT security manager for a video game software development company. Which of the following is most likely to be your primary concern on a daily basis?
Response:

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

Answer: C

NEW QUESTION 197
- (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 200
- (Exam Topic 2)
Administrative penalties for violating the General Data Protection Regulation (GDPR) can range up to
_____ .
Response:

A. US$100,000
B. 500,000 euros
C. 20,000,000 euros
D. 1,000,000 euros

Answer: C

NEW QUESTION 202
- (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 205
- (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 207
- (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 208
- (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 209
- (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 213
- (Exam Topic 2)
Why does the physical location of your data backup and/or BCDR failover environment matter? Response:

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

Answer: A

NEW QUESTION 217
- (Exam Topic 2)
Which type of software is most likely to be reviewed by the most personnel, with the most varied perspectives?
Response:

A. Database management software
B. Open source software
C. Secure software
D. Proprietary software

Answer: B

NEW QUESTION 219
- (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 220
- (Exam Topic 2)
Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?
Response:

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

Answer: C

NEW QUESTION 222
- (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 224
- (Exam Topic 2)
In the cloud motif, the data processor is usually: Response:

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

Answer: C

NEW QUESTION 228
- (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 229
- (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 233
- (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 235
- (Exam Topic 2)
What is a cloud storage architecture that manages the data in a hierarchy of files? Response:

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

Answer: B

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

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

Answer: B

NEW QUESTION 243
- (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 247
- (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 251
- (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 256
- (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 258
- (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 263
- (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 264
- (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 269
- (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 271
- (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 276
- (Exam Topic 2)
The Restatement (Second) Conflict of Law refers to which of the following? Response:

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

Answer: A

NEW QUESTION 280
- (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 281
- (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 282
- (Exam Topic 2)
You have been tasked by management to offload processing and validation of incoming encoded data from your application servers and their associated APIs.
Which of the following would be the most appropriate device or software to consider?
Response:

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

Answer: A

NEW QUESTION 283

- (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 284
- (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 286
- (Exam Topic 2)
_____ can often be the result of inadvertent activity. Response:

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

Answer: C

NEW QUESTION 290
- (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 291
- (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 295
- (Exam Topic 2)
Your organization is developing software for wide use by the public. You have decided to test it in a cloud environment, in a PaaS model. Which of the following should be of particular concern to your organization for this situation?
Response:

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

Answer: B

NEW QUESTION 299
- (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 302
- (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 305
- (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 310
- (Exam Topic 2)
Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality? Response:

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

Answer: C

NEW QUESTION 312
- (Exam Topic 2)
Designers making applications for the cloud have to take into consideration risks and operational constraints that did not exist or were not as pronounced in the legacy environment.
Which of the following is an element cloud app designers may have to consider incorporating in software for the cloud that might not have been as important in the legacy environment?
Response:

A. IAM capability
B. DDoS resistance
C. Encryption for data at rest and in motion
D. Field validation

Answer: C

NEW QUESTION 315
- (Exam Topic 2)
From a security perspective, automation of configuration aids in _____.
Response:

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

Answer: B

NEW QUESTION 320
- (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 324
- (Exam Topic 3)
You work for a company that operates a production environment in the cloud. Another company using the same cloud provider is under investigation by law enforcement for racketeering.
Your company should be concerned about this because of the cloud characteristic of . Response:

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

Answer: B

NEW QUESTION 329
- (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 333
- (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 335
- (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 338
- (Exam Topic 3)
Access should be based on _____.
Response:

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

Answer: B

NEW QUESTION 342
- (Exam Topic 3)
Digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM) often protect unauthorized distribution of what type of intellectual property?
Response:

A. Patents
B. Trademarks
C. Personally identifiable information (PII)
D. Copyright

Answer: D

NEW QUESTION 344
- (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 345
- (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 348
- (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 349
- (Exam Topic 3)
Digital rights management (DRM) tools can be combined with _____, to enhance security capabilities. Response:

A. Roaming identity services (RIS)
B. Egress monitoring solutions (DLP)
C. Internal hardware settings (BIOS)
D. Remote Authentication Dial-In User Service (RADIUS)

Answer: B

NEW QUESTION 352
- (Exam Topic 3)
When a customer performs a penetration test in the cloud, why isn't the test an optimum simu-lation of attack conditions?
Response:

A. Attackers don't use remote access for cloud activity
B. Advanced notice removes the element of surprise
C. When cloud customers use malware, it's not the same as when attackers use malware
D. Regulator involvement changes the attack surface

Answer: B

NEW QUESTION 353
- (Exam Topic 3)
Patches do all the following except _____.
Response:

A. Address newly discovered vulnerabilities
B. Solve cloud interoperability problems
C. Add new features and capabilities to existing systems
D. Address performance issues

Answer: B

NEW QUESTION 355
- (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 359
- (Exam Topic 3)
Which of the following data-sanitation approaches are always available within a cloud environment? Response:

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

Answer: D

NEW QUESTION 360
- (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 362
- (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 365
- (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 370
- (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 373
- (Exam Topic 3)
DLP solutions can aid in deterring loss due to which of the following?
Response:

A. Randomization
B. Inadvertent disclosure
C. Natural disaster
D. Device failure

Answer: B

NEW QUESTION 376
- (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 379
- (Exam Topic 3)
Which theoretical technology would allow superposition of physical states to increase both computing capacity and encryption keyspace?
Response:

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

Answer: B

NEW QUESTION 384
- (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 386
- (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 388
- (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 390
- (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 393

- (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 398
- (Exam Topic 3)
There are two reasons to conduct a test of the organization's recovery from backup in an environment other
than the primary production environment. Which of the following is one of them? Response:

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

Answer: B

NEW QUESTION 399
- (Exam Topic 3)
Which of the following methods of addressing risk is most associated with insurance? Response:

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

Answer: A

NEW QUESTION 403
- (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 408
- (Exam Topic 3)
Which ISO/IEC standards set documents the cloud definitions for staffing and official roles? Response:

A. ISO/IEC 27001
B. ISO/IEC 17788
C. ISO/IEC 17789
D. ISO/IEC 27040

Answer: B

NEW QUESTION 413
- (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 416
- (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 420
- (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 425
- (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 429
- (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 434
- (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 439
- (Exam Topic 3)
Security best practices in a virtualized network environment would include which of the following? Response:

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

Answer: A

NEW QUESTION 442
- (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 446
- (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 450
- (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 453
- (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 454
- (Exam Topic 3)
The BIA can be used to provide information about all the following, except: Response:

A. Risk analysis
B. Secure acquisition
C. BC/DR planning
D. Selection of security controls

Answer: B

NEW QUESTION 458
- (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 462
- (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 464
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your CCSP Exam with Our Prep Materials Via below:

https://www.certleader.com/CCSP-dumps.html