ISC2

Exam Questions CCSP

Certified Cloud Security Professional

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

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

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
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 3
- (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 4
- (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 5
- (Exam Topic 1)
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing?
Response:

A. Cloud customers and third parties are continually enhancing and modifying APIs.
B. APIs can have automated settings.
C. It is impossible to uninstall APIs.
D. APIs are a form of malware.

Answer: A

NEW QUESTION 6
- (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 7
- (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 8
- (Exam Topic 1)
Which concept of cloud computing pertains to the ability to reuse components and services of an application for other purposes?

A. Portability
B. Interoperability
C. Resource pooling
D. Elasticity

Answer: B

NEW QUESTION 9
- (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 10
- (Exam Topic 1)
Of the following, which is probably the most significant risk in a managed cloud environment? Response:

A. DDoS
B. Management plane breach
C. Guest escape
D. Physical attack on the utility service lines

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
Which document will enforce uptime and availability requirements between the cloud customer and cloud provider?
Response:

A. Contract
B. Operational level agreement
C. Service level agreement
D. Regulation

Answer: C

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

A. A method where the last few numbers in a dataset are not obscure
B. These are often used for authentication.
C. A method for creating similar but inauthentic datasets used for software testing and user training.
D. A method used to protect prying eyes from data such as social security numbers and credit card data.
E. Data masking involves stripping out all similar digits in a string of numbers so as to obscure the original number.

Answer: B

NEW QUESTION 13
- (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 16
- (Exam Topic 1)
Which of the following are contractual components that the CSP should review and understand fully when contracting with a cloud service provider? (Choose two.)

A. Concurrently maintainable site infrastructure
B. Use of subcontractors
C. Redundant site infrastructure capacity components
D. Scope of processing

Answer: BD

NEW QUESTION 19
- (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 23
- (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 27
- (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 30
- (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 35
- (Exam Topic 1)
Because PaaS implementations are so often used for software development, what is one of the vulnerabilities that should always be kept in mind?
Response:

A. Malware
B. Loss/theft of portable devices
C. Backdoors
D. DoS/DDoS

Answer: C

NEW QUESTION 36
- (Exam Topic 1)
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 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.
What should you not expect the tool to address? Response:

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

Answer: B

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

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

Answer: B

NEW QUESTION 43
- (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 45
- (Exam Topic 1)
Every cloud service provider that opts to join the CSA STAR program registry must complete a _____.

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

Answer: B

NEW QUESTION 49
- (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 51
- (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 55
- (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 58
- (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 59
- (Exam Topic 1)
DAST checks software functionality in _____.
Response:

A. The production environment
B. A runtime state
C. The cloud
D. An IaaS configuration

Answer: B

NEW QUESTION 64
- (Exam Topic 1)
A firewall can use all of the following techniques for controlling traffic except:

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

Answer: D

NEW QUESTION 69
- (Exam Topic 1)
When a data center is configured such that the backs of the devices face each other and the ambient temperature in the work area is cool, it is called _____.
Response:

A. Hot aisle containment
B. Cold aisle containment
C. Thermo-optimized
D. HVAC modulated

Answer: A

NEW QUESTION 70
- (Exam Topic 1)
One of the security challenges of operating in the cloud is that additional controls must be placed on file storage systems because _____ .
Response:

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

Answer: D

NEW QUESTION 71
- (Exam Topic 1)

Which type of report is considered for “general” use and does not contain any sensitive information? Response:

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

Answer: C

NEW QUESTION 72
- (Exam Topic 1)
Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:
Response:

A. The cloud provider’s suppliers
B. The cloud provider’s vendors
C. The cloud provider’s utilities
D. The cloud provider’s resellers

Answer: D

NEW QUESTION 77
- (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 78
- (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, 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 84
- (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 87
- (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 92
- (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 96
- (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 99
- (Exam Topic 1)
A honeypot should contain data_____.
Response:

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

Answer: C

NEW QUESTION 100
- (Exam Topic 1)
Who will determine data classifications for the cloud customer?

A. The cloud provider
B. NIST
C. Regulators
D. The cloud customer

Answer: D

NEW QUESTION 103
- (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 106
- (Exam Topic 1)
Application virtualization can typically be used for .

A. Denying access to untrusted users
B. Detecting and mitigating DDoS attacks
C. Replacing encryption as a necessary control
D. Running an application on an endpoint without installing it

Answer: D

NEW QUESTION 110
- (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 113
- (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 116
- (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 117
- (Exam Topic 1)
At which layer does the IPSec protocol operate to encrypt and protect communications between two parties? Response:

A. Network
B. Application
C. Transport
D. Data link

Answer: A

NEW QUESTION 118
- (Exam Topic 2)
While an audit is being conducted, which of the following could cause management and the auditors to change the original plan in order to continue with the audit? Response:

A. Cost overruns
B. Impact on systems
C. Regulatory changes
D. Software version changes

Answer: A

NEW QUESTION 119
- (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 123
- (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 125
- (Exam Topic 2)
Which of the following is the best example of a key component of regulated PII? Response:

A. Items that should be implemented
B. Mandatory breach reporting
C. Audit rights of subcontractors
D. PCI DSS

Answer: B

NEW QUESTION 130
- (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 132
- (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 135
- (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 136
- (Exam Topic 2)
You are the security director for a chain of automotive repair centers across several states. Your company uses a cloud SaaS provider, for business functions that cross several of the locations of your facilities, such as: 1) ordering parts 2) logistics and inventory 3) billing, and 4) marketing.
The manager at one of your newest locations reports that there is a competing car repair company that has a logo that looks almost exactly like the one your company uses. What will most likely affect the determination of who has ownership of the logo?
Response:

A. Whoever first used the logo
B. The jurisdiction where both businesses are using the logo simultaneously
C. Whoever first applied for legal protection of the logo
D. Whichever entity has the most customers that recognize the logo

Answer: C

NEW QUESTION 139
- (Exam Topic 2)
In a cloud environment, encryption should be used for all the following, except: Response:

A. Long-term storage of data
B. Near-term storage of virtualized images
C. Secure sessions/VPN
D. Profile formatting

Answer: D

NEW QUESTION 144
- (Exam Topic 2)
The physical layout of a cloud data center campus should include redundancies of all the following except _____ .
Response:

A. Physical perimeter security controls (fences, lights, walls, etc.)
B. The administration/support staff building
C. Electrical utility lines
D. Communications connectivity lines

Answer: B

NEW QUESTION 147
- (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 148
- (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 149
- (Exam Topic 2)
A cloud data encryption situation where the cloud customer retains control of the encryption keys and the cloud provider only processes and stores the data could be considered a _____.
Response:

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

Answer: C

NEW QUESTION 152
- (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 154
- (Exam Topic 2)
Which of the following would NOT be included as input into the requirements gathering for an application or system?
Response:

A. Users
B. Management
C. Regulators
D. Auditors

Answer: D

NEW QUESTION 155
- (Exam Topic 2)
Resolving resource contentions in the cloud will most likely be the job of the _____.
Response:

A. Router
B. Emulator
C. Regulator

D. Hypervisor

Answer: D

NEW QUESTION 160
- (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 162
- (Exam Topic 2)
What is the most secure form of code testing and review? Response:

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

Answer: D

NEW QUESTION 164
- (Exam Topic 2)
In application-level encryption, where does the encryption engine reside? Response:

A. In the application accessing the database
B. In the OS on which the application is run
C. Within the database accessed by the application
D. In the volume where the database resides

Answer: A

NEW QUESTION 165
- (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 169
- (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 174
- (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 176
- (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 179
- (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 180
- (Exam Topic 2)
What is a form of cloud storage where data is stored as objects, arranged in a hierarchal structure, like a file tree?
Response:

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

Answer: D

NEW QUESTION 184
- (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 189
- (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 191
- (Exam Topic 2)
Which of the following is a risk associated with manual patching especially in the cloud?
Response:

A. No notice before the impact is realized
B. Lack of applicability to the environment
C. Patches may or may not address the vulnerability they were designed to fix.
D. The possibility for human error

Answer: D

NEW QUESTION 194
- (Exam Topic 2)
All of the following might be used as data discovery characteristics in a content-analysis-based data discovery effort except _____.
Response:

A. Keywords

B. Pattern-matching
C. Frequency
D. Inheritance

Answer: D

NEW QUESTION 195
- (Exam Topic 2)
Federation should be _____ to the users.
Response:

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

Answer: C

NEW QUESTION 200
- (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 203
- (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 208
- (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 213
- (Exam Topic 2)
What is a cloud storage architecture that manages the data in caches of copied content close to locations of high demand?
Response:

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

Answer: D

NEW QUESTION 218
- (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 221
- (Exam Topic 2)
_____ can often be the result of inadvertent activity. Response:

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

Answer: C

NEW QUESTION 223
- (Exam Topic 2)
You are the IT director for a small contracting firm. Your company is considering migrating to a cloud production environment.
Which service model would best fit your needs if you wanted an option that reduced the chance of vendor lock-in but also did not require the highest degree of administration by your own personnel?
Response:

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

Answer: B

NEW QUESTION 225
- (Exam Topic 2)
Which of the following data protection methodologies maintains the ability to connect back values to the original values?
Response:

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

Answer: A

NEW QUESTION 226
- (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 231
- (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 235
- (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 237
- (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 241
- (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 242
- (Exam Topic 3)
The BCDR plan/process should be written and documented in such a way that it can be used by _____.
Response:

A. Users
B. Essential BCDR team members
C. Regulators
D. Someone with the requisite skills

Answer: D

NEW QUESTION 246
- (Exam Topic 3)
Which kind of SSAE report comes with a seal of approval from a certified auditor? Response:

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

Answer: C

NEW QUESTION 251
- (Exam Topic 3)
Which of the following methods for the safe disposal of electronic records can always be used in a cloud environment? Response:

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

Answer: B

NEW QUESTION 256
- (Exam Topic 3)
Devices in the cloud datacenter should be secure against attack. All the following are means of hardening devices, except:
Response:

A. Using a strong password policy
B. Removing default passwords
C. Strictly limiting physical access
D. Removing all admin accounts

Answer: D

NEW QUESTION 259
- (Exam Topic 3)
The Brewer-Nash security model is also known as which of the following? Response:

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

D. RBAC

Answer: B

NEW QUESTION 263
- (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 264
- (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 269
- (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 274
- (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 276
- (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 277
- (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 281
- (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 286
- (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 288
- (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 289
- (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 293
- (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 296
- (Exam Topic 3)
Virtual machine (VM) configuration management (CM) tools should probably include _____.
Response:

A. Biometric recognition
B. Anti-tampering mechanisms
C. Log file generation
D. Hackback capabilities

Answer: C

NEW QUESTION 299
- (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 303
- (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 306
- (Exam Topic 3)
Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like: Response:

A. Syn floods
B. Ransomware
C. XSS and SQL injection
D. Password cracking

Answer: C

NEW QUESTION 307
- (Exam Topic 3)
Tokenization requires two distinct _____.
Response:

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

Answer: B

NEW QUESTION 310
- (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 314
- (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 319
- (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 320

- (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 321
- (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 325
- (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 327
- (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 329
- (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 332
- (Exam Topic 3)
_____ is perhaps the main external factor driving IAM efforts. Response:

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

Answer: A

NEW QUESTION 335
- (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 338
- (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 343
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CCSP Practice Exam Features:

* CCSP Questions and Answers Updated Frequently

* CCSP Practice Questions Verified by Expert Senior Certified Staff

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

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