ISC2

Exam Questions CCSP

Certified Cloud Security Professional

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

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

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
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)
All of the following are usually nonfunctional requirements except _____.
Response:

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

Answer: D

NEW QUESTION 5
- (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 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)
When an organization implements an SIEM solution and begins aggregating event data, the configured event sources are only valid at the time it was configured.
Application modifications, patching, and other upgrades will change the events generated and how they are represented over time.
What process is necessary to ensure events are collected and processed with this in mind?

A. Continual review
B. Continuous optimization
C. Aggregation updates
D. Event elasticity

Answer: B

NEW QUESTION 8
- (Exam Topic 1)
Which of the following should occur at each stage of the SDLC?

A. Added functionality
B. Management review
C. Verification and validation
D. Repurposing of any newly developed components

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
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 10
- (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)
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 15
- (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 17
- (Exam Topic 1)
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.
Which of the following benefits will the CSA CCM offer your organization? Response:

A. Simplifying regulatory compliance
B. Collecting multiple data streams from your log files
C. Ensuring that the baseline configuration is applied to all systems
D. Enforcing contract terms between your organization and the cloud provider

Answer: A

NEW QUESTION 22
- (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 24
- (Exam Topic 1)
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
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 27
- (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 32
- (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 35
- (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)
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 45
- (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 47
- (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 51
- (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 52
- (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 57
- (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 60
- (Exam Topic 1)
Which Common Criteria Evaluation Assurance Level (EAL) is granted to those products that are formally verified in terms of design and tested by an independent third party?

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

Answer: D

NEW QUESTION 62
- (Exam Topic 1)
One of the security challenges of operating in the cloud is that additional controls must be placed on file storage systems because _____ .
Response:

A. File stores are always kept in plain text in the cloud
B. There is no way to sanitize file storage space in the cloud

C. Virtualization necessarily prevents the use of application-based security controls
D. Virtual machines are stored as snapshotted files when not in use

Answer: D

NEW QUESTION 67
- (Exam Topic 1)
Which 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 69
- (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 70
- (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 71
- (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 74
- (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 79
- (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 81
- (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 83
- (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 86
- (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 89
- (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 93
- (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 96
- (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 98
- (Exam Topic 1)
When using transparent encryption of a database, where does the encryption engine reside? Response:

A. At the application using the database
B. On the instance(s) attached to the volume
C. In a key management system
D. Within the database

Answer: D

NEW QUESTION 99
- (Exam Topic 2)
What could be the result of failure of the cloud provider to secure the hypervisor in such a way that one user on a virtual machine can see the resource calls of another user's virtual machine?
Response:

A. Unauthorized data disclosure
B. Inference attacks
C. Social engineering
D. Physical intrusion

Answer: B

NEW QUESTION 104
- (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 107
- (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 112
- (Exam Topic 2)
You are the data manager for a retail company; you anticipate a much higher volume of sales activity in the final quarter of each calendar year than the other quarters.
In order to handle these increased transactions, and to accommodate the temporary sales personnel you will hire for only that time period, you consider augmenting your internal, on-premises production environment with a cloud capability for a specific duration, and will return to operating fully on-premises after the period of increased activity.
This is an example of _____.
Response:

A. Cloud framing
B. Cloud enhancement
C. Cloud fragility
D. Cloud bursting

Answer: D

NEW QUESTION 114
- (Exam Topic 2)
A bare-metal hypervisor is Type _____.
Response:

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

Answer: A

NEW QUESTION 117
- (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 121
- (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 124
- (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 125
- (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 129
- (Exam Topic 2)
Although encryption can help an organization to effectively decrease the possibility of data breaches, which other type of threat can it increase the chances of?
Response:

A. Insecure interfaces
B. Data loss
C. System vulnerabilities
D. Account hijacking

Answer: B

NEW QUESTION 134
- (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 138
- (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 142

- (Exam Topic 2)
Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?
Response:

A. Unvalidated redirects and forwards
B. Cross-site request forgery
C. Cross-site scripting
D. Insecure direct object references

Answer: A

NEW QUESTION 143
- (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 146
- (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 150
- (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 155
- (Exam Topic 2)
What is the risk to the organization posed by dashboards that display data discovery results? Response:

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

Answer: B

NEW QUESTION 156
- (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 159

- (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 162
- (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 163
- (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 165
- (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 166
- (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 169
- (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 173
- (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 174
- (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 179
- (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 184
- (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 189
- (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 191
- (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 193
- (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 197

- (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 198
- (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 201
- (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 202
- (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 206
- (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 210
- (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 214
- (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 219
- (Exam Topic 2)
When designing a cloud data center, which of the following aspects is not necessary to ensure continuity of operations during contingency operations?
Response:

A. Access to clean water
B. Broadband data connection
C. Extended battery backup
D. Physical access to the data center

Answer: C

NEW QUESTION 220
- (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 225
- (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 230
- (Exam Topic 2)
A denial of service (DoS) attack can potentially impact all customers within a cloud environment with the continued allocation of additional resources. Which of the following can be useful for a customer to protect themselves from a DoS attack against another customer?
Response:

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

Answer: B

NEW QUESTION 232
- (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 237
- (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 238
- (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 240
- (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 242
- (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 245
- (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 246
- (Exam Topic 2)
Which of the following is not a way to manage risk? Response:

A. Enveloping
B. Mitigating
C. Accepting
D. Transferring

Answer: A

NEW QUESTION 247
- (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 250
- (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 251
- (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 253
- (Exam Topic 3)
Why might an organization choose to comply with the ISO 27001 standard?
Response:

A. Price
B. Ease of implementation
C. International acceptance
D. Speed

Answer: C

NEW QUESTION 254
- (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 256
- (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 260
- (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 263
- (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 268
- (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 271
- (Exam Topic 3)
If bit-splitting is used to store data sets across multiple jurisdictions, how may this enhance security? Response:

A. By making seizure of data by law enforcement more difficult
B. By hiding it from attackers in a specific jurisdiction
C. By ensuring that users can only accidentally disclose data to one geographic area
D. By restricting privilege user access

Answer: A

NEW QUESTION 276
- (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 280
- (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 282
- (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 287
- (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 290
- (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 292
- (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 294
- (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 299
- (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 302
- (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 303
- (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 305
- (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 309
- (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 310
- (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 312
- (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 316
- (Exam Topic 3)
Dynamic application security testing (DAST) is usually considered a _____ form of testing. Response:
White-box

A. Parched field
B. Black-box
C. Gray-box
D. Parched field

Answer: B

NEW QUESTION 320
- (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 323
- (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 328
- (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 331
- (Exam Topic 3)
A web application firewall (WAF) can understand and act on _____ traffic.
Response:

A. Malicious
B. SMTP
C. ICMP
D. HTTP

Answer: D

NEW QUESTION 332
- (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 336
- (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 337
- (Exam Topic 3)
With cloud computing crossing many jurisdictional boundaries, it is a virtual certainty that conflicts will arise between differing regulations. What is the major impediment to resolving conflicts between multiple jurisdictions to form an overall policy?
Response:

A. Language differences
B. Technologies used
C. Licensing issues
D. Lack of international authority

Answer: D

NEW QUESTION 338
- (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 340
- (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 341
- (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 346
......

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
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)
All of the following are usually nonfunctional requirements except _____.
Response:

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

Answer: D

NEW QUESTION 5
- (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 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)
When an organization implements an SIEM solution and begins aggregating event data, the configured event sources are only valid at the time it was configured.
Application modifications, patching, and other upgrades will change the events generated and how they are represented over time.
What process is necessary to ensure events are collected and processed with this in mind?

A. Continual review
B. Continuous optimization
C. Aggregation updates
D. Event elasticity

Answer: B

NEW QUESTION 8
- (Exam Topic 1)
Which of the following should occur at each stage of the SDLC?

A. Added functionality
B. Management review
C. Verification and validation
D. Repurposing of any newly developed components

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
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 10
- (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)
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 15
- (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 17
- (Exam Topic 1)
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.
Which of the following benefits will the CSA CCM offer your organization? Response:

A. Simplifying regulatory compliance
B. Collecting multiple data streams from your log files
C. Ensuring that the baseline configuration is applied to all systems
D. Enforcing contract terms between your organization and the cloud provider

Answer: A

NEW QUESTION 22
- (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 24
- (Exam Topic 1)
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
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 27
- (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 32
- (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 35
- (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)
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 45
- (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 47
- (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 51
- (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 52
- (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 57
- (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 60
- (Exam Topic 1)
Which Common Criteria Evaluation Assurance Level (EAL) is granted to those products that are formally verified in terms of design and tested by an independent third party?

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

Answer: D

NEW QUESTION 62
- (Exam Topic 1)
One of the security challenges of operating in the cloud is that additional controls must be placed on file storage systems because _____ .
Response:

A. File stores are always kept in plain text in the cloud
B. There is no way to sanitize file storage space in the cloud

C. Virtualization necessarily prevents the use of application-based security controls
D. Virtual machines are stored as snapshotted files when not in use

Answer: D

NEW QUESTION 67
- (Exam Topic 1)
Which 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 69
- (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 70
- (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 71
- (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 74
- (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 79
- (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 81
- (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 83
- (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 86
- (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 89
- (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 93
- (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 96
- (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 98
- (Exam Topic 1)
When using transparent encryption of a database, where does the encryption engine reside? Response:

A. At the application using the database
B. On the instance(s) attached to the volume
C. In a key management system
D. Within the database

Answer: D

NEW QUESTION 99
- (Exam Topic 2)
What could be the result of failure of the cloud provider to secure the hypervisor in such a way that one user on a virtual machine can see the resource calls of another user's virtual machine?
Response:

A. Unauthorized data disclosure
B. Inference attacks
C. Social engineering
D. Physical intrusion

Answer: B

NEW QUESTION 104
- (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 107
- (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 112
- (Exam Topic 2)
You are the data manager for a retail company; you anticipate a much higher volume of sales activity in the final quarter of each calendar year than the other quarters.
In order to handle these increased transactions, and to accommodate the temporary sales personnel you will hire for only that time period, you consider augmenting your internal, on-premises production environment with a cloud capability for a specific duration, and will return to operating fully on-premises after the period of increased activity.
This is an example of _____.
Response:

A. Cloud framing
B. Cloud enhancement
C. Cloud fragility
D. Cloud bursting

Answer: D

NEW QUESTION 114
- (Exam Topic 2)
A bare-metal hypervisor is Type _____.
Response:

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

Answer: A

NEW QUESTION 117
- (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 121
- (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 124
- (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 125
- (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 129
- (Exam Topic 2)
Although encryption can help an organization to effectively decrease the possibility of data breaches, which other type of threat can it increase the chances of?
Response:

A. Insecure interfaces
B. Data loss
C. System vulnerabilities
D. Account hijacking

Answer: B

NEW QUESTION 134
- (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 138
- (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 142

- (Exam Topic 2)
Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?
Response:

A. Unvalidated redirects and forwards
B. Cross-site request forgery
C. Cross-site scripting
D. Insecure direct object references

Answer: A

NEW QUESTION 143
- (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 146
- (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 150
- (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 155
- (Exam Topic 2)
What is the risk to the organization posed by dashboards that display data discovery results? Response:

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

Answer: B

NEW QUESTION 156
- (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 159

- (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 162
- (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 163
- (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 165
- (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 166
- (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 169
- (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 173
- (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 174
- (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 179
- (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 184
- (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 189
- (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 191
- (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 193
- (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 197

- (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 198
- (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 201
- (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 202
- (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 206
- (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 210
- (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 214
- (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 219
- (Exam Topic 2)
When designing a cloud data center, which of the following aspects is not necessary to ensure continuity of operations during contingency operations?
Response:

A. Access to clean water
B. Broadband data connection
C. Extended battery backup
D. Physical access to the data center

Answer: C

NEW QUESTION 220
- (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 225
- (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 230
- (Exam Topic 2)
A denial of service (DoS) attack can potentially impact all customers within a cloud environment with the continued allocation of additional resources. Which of the following can be useful for a customer to protect themselves from a DoS attack against another customer?
Response:

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

Answer: B

NEW QUESTION 232
- (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 237
- (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 238
- (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 240
- (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 242
- (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 245
- (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 246
- (Exam Topic 2)
Which of the following is not a way to manage risk? Response:

A. Enveloping
B. Mitigating
C. Accepting
D. Transferring

Answer: A

NEW QUESTION 247
- (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 250
- (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 251
- (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 253
- (Exam Topic 3)
Why might an organization choose to comply with the ISO 27001 standard?
Response:

A. Price
B. Ease of implementation
C. International acceptance
D. Speed

Answer: C

NEW QUESTION 254
- (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 256
- (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 260
- (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 263
- (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 268
- (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 271
- (Exam Topic 3)
If bit-splitting is used to store data sets across multiple jurisdictions, how may this enhance security? Response:

A. By making seizure of data by law enforcement more difficult
B. By hiding it from attackers in a specific jurisdiction
C. By ensuring that users can only accidentally disclose data to one geographic area
D. By restricting privilege user access

Answer: A

NEW QUESTION 276
- (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 280
- (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 282
- (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 287
- (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 290
- (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 292
- (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 294
- (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 299
- (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 302
- (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 303
- (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 305
- (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 309
- (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 310
- (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 312
- (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 316
- (Exam Topic 3)
Dynamic application security testing (DAST) is usually considered a _____ form of testing. Response:
White-box

A. Parched field
B. Black-box
C. Gray-box
D. Parched field

Answer: B

NEW QUESTION 320
- (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 323
- (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 328
- (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 331
- (Exam Topic 3)
A web application firewall (WAF) can understand and act on _____ traffic.
Response:

A. Malicious
B. SMTP
C. ICMP
D. HTTP

Answer: D

NEW QUESTION 332
- (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 336
- (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 337
- (Exam Topic 3)
With cloud computing crossing many jurisdictional boundaries, it is a virtual certainty that conflicts will arise between differing regulations. What is the major impediment to resolving conflicts between multiple jurisdictions to form an overall policy?
Response:

A. Language differences
B. Technologies used
C. Licensing issues
D. Lack of international authority

Answer: D

NEW QUESTION 338
- (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 340
- (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 341
- (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 346
......

Relate Links

100% Pass Your CCSP Exam with Exambible Prep Materials

https://www.exambible.com/CCSP-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/