

ISC2

Exam Questions CCSP

Certified Cloud Security Professional



NEW QUESTION 1

- (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 2

- (Exam Topic 1)

Which strategy involves using a fake production system to lure attackers in order to learn about their tactics?

Response:

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

Answer: B

NEW QUESTION 3

- (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 4

- (Exam Topic 1)

What is the federal agency that accepts applications for new patents?

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

Answer: B

NEW QUESTION 5

- (Exam Topic 1)

Which of the following is a file server that provides data access to multiple, heterogeneous machines/users on the network?

Response:

- A. Storage area network (SAN)
- B. Network-attached storage (NAS)
- C. Hardware security module (HSM)
- D. Content delivery network (CDN)

Answer: B

NEW QUESTION 6

- (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 7

- (Exam Topic 1)

A typical DLP tool can enhance the organization's efforts at accomplishing what legal task? Response:

- A. Evidence collection
- B. Delivering testimony
- C. Criminal prosecution
- D. Enforcement of intellectual property rights

Answer: A

NEW QUESTION 8

- (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 9

- (Exam Topic 1)

Egress monitoring solutions usually include a function that _____.
Response:

- A. Uses biometrics to scan users
- B. Inspects incoming packets
- C. Resides on client machines
- D. Uses stateful inspection

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 10

- (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 15

- (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 20

- (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 22

- (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 25

- (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 28

- (Exam Topic 1)

The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “cross-site scripting (XSS).” Which of the following is not a method for reducing the risk of XSS attacks? Response:

- A. Use an auto-escaping template system.
- B. XML escape all identity assertions.
- C. Sanitize HTML markup with a library designed for the purpose.
- D. HTML escape JSON values in an HTML context and read the data with JSON.parse.

Answer: B

NEW QUESTION 31

- (Exam Topic 1)

The cloud deployment model that features joint ownership of assets among an affinity group is known as: Response:

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

Answer: D

NEW QUESTION 32

- (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 37

- (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 40

- (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 45

- (Exam Topic 1)

TLS uses _____ to authenticate a connection and create a shared secret for the duration of the session.

- A. SAML 2.0
- B. X.509 certificates
- C. 802.11X
- D. The Diffie-Hellman process

Answer: B

NEW QUESTION 49

- (Exam Topic 1)

In the cloud motif, the data processor is usually: Response:

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

Answer: C

NEW QUESTION 50

- (Exam Topic 1)

A honeypot can be used for all the following purposes except _____.

Response:

- A. Gathering threat intelligence
- B. Luring attackers
- C. Distracting attackers
- D. Delaying attackers

Answer: B

NEW QUESTION 53

- (Exam Topic 1)

Which security certification serves as a general framework that can be applied to any type of system or application?

- A. ISO/IEC 27001
- B. PCI DSS
- C. FIPS 140-2
- D. NIST SP 800-53

Answer: A

NEW QUESTION 58

- (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 63

- (Exam Topic 1)

All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:

Response:

- A. Tokenization

- B. Data discovery
- C. Obfuscation
- D. Masking

Answer: B

NEW QUESTION 68

- (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 71

- (Exam Topic 1)

The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “sensitive data exposure.” Which of these is a technique to reduce the potential for a sensitive data exposure? Response:

- A. Extensive user training on proper data handling techniques
- B. Advanced firewalls inspecting all inbound traffic, to include content-based screening
- C. Ensuring the use of utility backup power supplies
- D. Roving security guards

Answer: A

NEW QUESTION 73

- (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 75

- (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 77

- (Exam Topic 1)

When an organization considers cloud migrations, the organization’s software developers will need to know which _____ and _____ which the organization will be using, in order to properly and securely create suitable applications.

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

Answer: C

NEW QUESTION 79

- (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 83

- (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 87

- (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 91

- (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 94

- (Exam Topic 1)

Which of the following is not a reason for conducting audits?

- A. Regulatory compliance
- B. User satisfaction
- C. Determination of service quality
- D. Security assurance

Answer: B

NEW QUESTION 95

- (Exam Topic 1)

Heating, ventilation, and air conditioning (HVAC) systems cool the data center by pushing warm air into _____.

Response:

- A. The server inlets
- B. Underfloor plenums
- C. HVAC intakes
- D. The outside world

Answer: D

NEW QUESTION 97

- (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 102

- (Exam Topic 1)

_____ is the most prevalent protocol used in identity federation.

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

Answer: B

NEW QUESTION 104

- (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 108

- (Exam Topic 1)

What are the six components that make up the STRIDE threat model? Response:

- A. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
- B. Spoofing, Tampering, Non-Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
- C. Spoofing, Tampering, Repudiation, Information Disclosure, Distributed Denial of Service, and Elevation of Privilege
- D. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Social Engineering

Answer: A

NEW QUESTION 110

- (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 113

- (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 118

- (Exam Topic 2)

What is the intellectual property protection for the logo of a new video game? Response:

- A. Copyright
- B. Patent
- C. Trademark
- D. Trade secret

Answer: C

NEW QUESTION 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 126

- (Exam Topic 2)

A process for _____ can aid in protecting against data disclosure due to lost devices. Response:

- A. User punishment
- B. Credential revocation

- C. Law enforcement notification
- D. Device tracking

Answer: B

NEW QUESTION 131

- (Exam Topic 2)

In a Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a _____.

Response:

- A. Domain name (DN)
- B. Distinguished name (DN)
- C. Directory name (DN)
- D. Default name (DN)

Answer: B

NEW QUESTION 133

- (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 134

- (Exam Topic 2)

Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?

Response:

- A. Persistence
- B. Influence
- C. Resistance
- D. Trepidation

Answer: A

NEW QUESTION 136

- (Exam Topic 2)

Which of the following is not one of the types of controls? Response:

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

Answer: A

NEW QUESTION 140

- (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 144

- (Exam Topic 2)

Which of the following is a method for apportioning resources that involves setting maximum usage amounts for all tenants/customers within the environment?

Response:

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

Answer: D

NEW QUESTION 145

- (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 149

- (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 151

- (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 155

- (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 159

- (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 162

- (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 167

- (Exam Topic 2)

Tokenization requires at least _____ database(s).

Response:

- A. One

- B. Two
- C. Three
- D. Four

Answer: B

NEW QUESTION 172

- (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 177

- (Exam Topic 2)

Your organization is considering a move to a cloud environment and is looking for certifications or audit reports from cloud providers to ensure adequate security controls and processes.

Which of the following is NOT a security certification or audit report that would be pertinent? Response:

- A. FedRAMP
- B. PCI DSS
- C. FIPS 140-2
- D. SOC Type 2

Answer: C

NEW QUESTION 180

- (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 182

- (Exam Topic 2)

All of the following are identity federation standards commonly found in use today except _____.

Response:

- A. WS-Federation
- B. OpenID
- C. OAuth
- D. PGP

Answer: D

NEW QUESTION 187

- (Exam Topic 2)

What are the phases of a software development lifecycle process model? Response:

- A. Planning and requirements analysis, define, design, develop, testing, and maintenance
- B. Define, planning and requirements analysis, design, develop, testing, and maintenance
- C. Planning and requirements analysis, define, design, testing, develop, and maintenance
- D. Planning and requirements analysis, design, define, develop, testing, and maintenance

Answer: A

NEW QUESTION 189

- (Exam Topic 2)

Which security certification serves as a general framework that can be applied to any type of system or application?

Response:

- A. ISO/IEC 27001
- B. PCI DSS
- C. FIPS 140-2
- D. NIST SP 800-53

Answer: A

NEW QUESTION 191

- (Exam Topic 2)

What type of software is often considered secured and validated via community knowledge?

Response:

- A. Proprietary
- B. Object-oriented
- C. Open source
- D. Scripting

Answer: C

NEW QUESTION 194

- (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 199

- (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 204

- (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 205

- (Exam Topic 2)

Which of the following is a possible negative aspect of bit-splitting? Response:

- A. It may require trust in additional third parties beyond the primary cloud service provider.
- B. There may be cause for management concern that the technology will violate internal policy.
- C. Users will have far greater difficulty understanding the implementation.
- D. Limited vendors make acquisition and support challenging.

Answer: A

NEW QUESTION 208

- (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 209

- (Exam Topic 2)

Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company's website)?

Response:

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

Answer: D

NEW QUESTION 213

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 216

- (Exam Topic 2)

_____ can often be the result of inadvertent activity. Response:

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

Answer: C

NEW QUESTION 220

- (Exam Topic 2)

Aside from the fact that the cloud customer probably cannot locate/reach the physical storage assets of the cloud provider, and that wiping an entire storage space would impact other customers, why would degaussing probably not be an effective means of secure sanitization in the cloud? Response:

- A. All the data storage space in the cloud is already gaussed.
- B. Cloud data storage may not be affected by degaussing.
- C. Federal law prohibits it in the United States.
- D. The blast radius is too wide.

Answer: B

NEW QUESTION 222

- (Exam Topic 2)

Which of the following is NOT a common component of a DLP implementation process? Response:

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

Answer: C

NEW QUESTION 224

- (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 226

- (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 231

- (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 234

- (Exam Topic 3)

Which technology is most associated with tunneling? Response:

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

Answer: B

NEW QUESTION 237

- (Exam Topic 3)

The nature of cloud computing and how it operates make complying with data discovery and disclosure orders more difficult. Which of the following concepts provides the biggest challenge in regard to data collection, pursuant to a legal order?

Response:

- A. Portability
- B. Multitenancy
- C. Reversibility
- D. Auto-scaling

Answer: B

NEW QUESTION 238

- (Exam Topic 3)

Which of the following aspects of the BC/DR process poses a risk to the organization? Response:

- A. Threat intelligence gathering
- B. Preplacement of response assets
- C. Budgeting for disaster
- D. Full testing of the plan

Answer: D

NEW QUESTION 239

- (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 240

- (Exam Topic 3)

Access should be based on _____.
Response:

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

Answer: B

NEW QUESTION 241

- (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 243

- (Exam Topic 3)

Cloud environments are based entirely on virtual machines and virtual devices, and those images are also in need of storage within the environment. What type of storage is typically used for virtual images?

Response:

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

Answer: D

NEW QUESTION 248

- (Exam Topic 3)

Which of the following would NOT be used to determine the classification of data?

Response:

- A. Metadata
- B. PII
- C. Creator
- D. Future use

Answer: D

NEW QUESTION 249

- (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 251

- (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 254

- (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 257

- (Exam Topic 3)

Which theoretical technology would allow superposition of physical states to increase both computing capacity and encryption keyspace?

Response:

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

Answer: B

NEW QUESTION 259

- (Exam Topic 3)

The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “injection.” In most cases, what is the method for reducing the risk of an injection attack? Response:

- A. User training
- B. Hardening the OS
- C. Input validation/bounds checking
- D. Physical locks

Answer: C

NEW QUESTION 260

- (Exam Topic 3)

Which of the following might make crypto-shredding difficult or useless? Response:

- A. Cloud provider also managing the organization's keys
- B. Lack of physical access to the environment
- C. External attackers
- D. Lack of user training and awareness

Answer: A

NEW QUESTION 264

- (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 269

- (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 272

- (Exam Topic 3)

It's important to maintain a current asset inventory list, including surveying your environment on a regular basis, in order to _____. Response:

- A. Prevent unknown, unpatched assets from being used as back doors to the environment
- B. Ensure that any lost devices are automatically entered into the acquisition system for repurchasing and replacement
- C. Maintain user morale by having their devices properly catalogued and annotated
- D. Ensure that billing for all devices is handled by the appropriate departments

Answer: A

NEW QUESTION 275

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 276

- (Exam Topic 3)

Tokenization requires two distinct _____.
Response:

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

Answer: B

NEW QUESTION 281

- (Exam Topic 3)

Which of the following is not a security concern related to archiving data for long-term storage? Response:

- A. Long-term storage of the related cryptographic keys
- B. Format of the data
- C. Media the data resides on
- D. Underground depth of the storage facility

Answer: D

NEW QUESTION 284

- (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 289

- (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 290

- (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 295

- (Exam Topic 3)

In a data retention policy, what is perhaps the most crucial element? Response:

- A. Location of the data archive
- B. Frequency of backups
- C. Security controls in long-term storage
- D. Data recovery procedures

Answer: D

NEW QUESTION 299

- (Exam Topic 3)

Your company has just been served with an eDiscovery order to collect event data and other pertinent information from your application during a specific period of time, to be used as potential evidence for a court proceeding.

Which of the following, apart from ensuring that you collect all pertinent data, would be the MOST important consideration?

Response:

- A. Encryption
- B. Chain of custody
- C. Compression
- D. Confidentiality

Answer: B

NEW QUESTION 304

- (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 307

- (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 310

- (Exam Topic 3)

What is the term used to describe loss of access to data because the cloud provider has ceased operation? Response:

- A. Closing
- B. Vendor lock-out
- C. Vendor lock-in
- D. Masking

Answer: B

NEW QUESTION 315

- (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 318

- (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 322

- (Exam Topic 3)

Bob is staging an attack against Alice's website. He is able to embed a link on her site that will execute malicious code on a visitor's machine, if the visitor clicks on the link. This is an example of which type of attack?

Response:

- A. Cross-site scripting
- B. Broken authentication/session management
- C. Security misconfiguration
- D. Insecure cryptographic storage

Answer: A

NEW QUESTION 326

.....

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

100% Actual & Verified — Instant Download, Please Click
[Order The CCSP Practice Test Here](#)