



ISC2

Exam Questions CCSP

Certified Cloud Security Professional

NEW QUESTION 1

- (Exam Topic 1)

What is the term that describes the situation when a malicious user/attacker can exit the restrictions of a single host and access other nodes on the network?

Response:

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

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

According to the (ISC)2 Cloud Secure Data Life Cycle, which phase comes soon after (or at the same time as) the Create phase?

- A. Store
- B. Use
- C. Deploy
- D. Archive

Answer: A

NEW QUESTION 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)

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)

The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing.

According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing?

Response:

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

Answer: A

NEW QUESTION 6

- (Exam Topic 1)

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 7

- (Exam Topic 1)

The cloud deployment model that features organizational ownership of the hardware and infrastructure, and usage only by members of that organization, is known as:

Response:

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

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

What is used with a single sign-on system for authentication after the identity provider has successfully authenticated a user?

Response:

- A. Token
- B. Key
- C. XML
- D. SAML

Answer: A

NEW QUESTION 9

- (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 10

- (Exam Topic 1)

Which phase of the cloud data lifecycle involves processing by a user or application? Response:

- A. Create
- B. Share
- C. Store
- D. Use

Answer: D

NEW QUESTION 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 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 20

- (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 24

- (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 27

- (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 31

- (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 34

- (Exam Topic 1)

You are performing an audit of the security controls used in a cloud environment. Which of the following would best serve your purpose?

Response:

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

Answer: B

NEW QUESTION 38

- (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 39

- (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 41

- (Exam Topic 1)

Cloud environments pose many unique challenges for a data custodian to properly adhere to policies and the use of data. What poses the biggest challenge for a data custodian with a PaaS implementation, over and above the same concerns with IaaS?

Response:

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

Answer: B

NEW QUESTION 43

- (Exam Topic 1)

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 48

- (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 52

- (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 57

- (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 61

- (Exam Topic 1)

Why are PaaS environments at a higher likelihood of suffering backdoor vulnerabilities?

- A. They rely on virtualization.
- B. They are often used for software development.
- C. They have multitenancy.
- D. They are scalable.

Answer: B

NEW QUESTION 64

- (Exam Topic 1)

You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider.

Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also allow users to select which APIs they install and use on their own devices in order to access and manipulate company data.

Of the following, what is a security control you'd like to implement to offset the risk(s) incurred by this practice?

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

Answer: A

NEW QUESTION 67

- (Exam Topic 1)

DAST checks software functionality in _____.

Response:

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

Answer: B

NEW QUESTION 70

- (Exam Topic 1)

Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:

Response:

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

Answer: D

NEW QUESTION 73

- (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 77

- (Exam Topic 1)

The physical layout of a cloud data center campus should include redundancies of all the following except

_____.

Response:

- A. Generators
- B. HVAC units
- C. Generator fuel storage
- D. Points of personnel ingress

Answer: D

NEW QUESTION 82

- (Exam Topic 1)

Log data should be protected _____.

Response:

- A. One level below the sensitivity level of the systems from which it was collected
- B. At least at the same sensitivity level as the systems from which it was collected
- C. With encryption in transit, at rest, and in use
- D. According to NIST guidelines

Answer: B

NEW QUESTION 85

- (Exam Topic 1)

Using one cloud provider for your operational environment and another for your BCDR backup will also give you the additional benefit of _____.

Response:

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

D. Lower cost

Answer: B

NEW QUESTION 86

- (Exam Topic 1)

Which concept pertains to cloud customers paying only for the resources they use and consume, and only for the duration they are using them?

Response:

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

Answer: A

NEW QUESTION 90

- (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 91

- (Exam Topic 1)

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 93

- (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 95

- (Exam Topic 1)

During which stage of the SDLC process should security be consulted and begin its initial involvement?

- A. Testing
- B. Design
- C. Development
- D. Requirement gathering

Answer: D

NEW QUESTION 100

- (Exam Topic 1)

Static software security testing typically uses _____ as a measure of how thorough the testing was. Response:

- A. Number of testers
- B. Flaws detected
- C. Code coverage
- D. Malware hits

Answer: C

NEW QUESTION 102

- (Exam Topic 1)

Which cloud service category offers the most customization options and control to the cloud customer?

Response:

- A. PaaS
- B. IaaS
- C. SaaS
- D. DaaS

Answer: B

NEW QUESTION 104

- (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 107

- (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 108

- (Exam Topic 2)

While an audit is being conducted, which of the following could cause management and the auditors to change the original plan in order to continue with the audit?

Response:

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

Answer: A

NEW QUESTION 112

- (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 116

- (Exam Topic 2)

You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.

Which of these activities should you perform before deploying the tool? Response:

- A. Survey your company's departments about the data under their control
- B. Reconstruct your firewalls
- C. Harden all your routers
- D. Adjust the hypervisors

Answer: A

NEW QUESTION 117

- (Exam Topic 2)

Which cloud service category brings with it the most expensive startup costs, but also the lowest costs for ongoing support and maintenance staff?

Response:

- A. IaaS
- B. SaaS
- C. PaaS
- D. DaaS

Answer: B

NEW QUESTION 121

- (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 122

- (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 123

- (Exam Topic 2)

A federated identity system is composed of three main components. Which of the following is NOT one of the three main components?

Response:

- A. Identity provider
- B. User
- C. Relying party
- D. API

Answer: D

NEW QUESTION 124

- (Exam Topic 2)

Which type of cloud service category would having a vendor-neutral encryption scheme for data at rest (DAR) be the MOST important?

Response:

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

Answer: B

NEW QUESTION 128

- (Exam Topic 2)

Your organization has made it a top priority that any cloud environment being considered to host production systems have guarantees that resources will always be available for allocation when needed.

Which of the following concepts will you need to ensure is part of the contract and SLA? Response:

- A. Limits
- B. Shares
- C. Resource pooling
- D. Reservations

Answer: D

NEW QUESTION 132

- (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 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)

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 136

- (Exam Topic 2)

Which one of the following is not one of the three common threat modeling techniques? Response:

- A. Focused on assets
- B. Focused on attackers
- C. Focused on software
- D. Focused on social engineering

Answer: D

NEW QUESTION 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 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 144

- (Exam Topic 2)

In a cloud environment, encryption should be used for all the following, except: Response:

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

Answer: D

NEW QUESTION 146

- (Exam Topic 2)

The physical layout of a cloud data center campus should include redundancies of all the following except _____.
Response:

- A. Physical perimeter security controls (fences, lights, walls, etc.)
- B. The administration/support staff building

- C. Electrical utility lines
- D. Communications connectivity lines

Answer: B

NEW QUESTION 149

- (Exam Topic 2)

Which of the following is NOT one of the cloud computing activities, as outlined in ISO/IEC 17789? Response:

- A. Cloud service provider
- B. Cloud service partner
- C. Cloud service administrator
- D. Cloud service customer

Answer: C

NEW QUESTION 153

- (Exam Topic 2)

All of the following entities 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 155

- (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 158

- (Exam Topic 2)

Although performing BCDR tests at regular intervals is a best practice to ensure processes and documentation are still relevant and efficient, which of the following represents a reason to conduct a BCDR review outside of the regular interval?

Response:

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

Answer: B

NEW QUESTION 162

- (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 167

- (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 170

- (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 in production 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 172

- (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 176

- (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 177

- (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 178

- (Exam Topic 2)

In application-level encryption, where does the encryption engine reside? Response:

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

Answer: A

NEW QUESTION 182

- (Exam Topic 2)

Which type of software is most likely to be reviewed by the most personnel, with the most varied perspectives?

Response:

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

Answer: B

NEW QUESTION 185

- (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 190

- (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 192

- (Exam Topic 2)

Single sign-on systems work by authenticating users from a centralized location or using a centralized method, and then allowing applications that trust the system to grant those users access. What would be passed between the authentication system and the applications to grant a user access?

Response:

- A. Ticket
- B. Certificate
- C. Credential
- D. Token

Answer: D

NEW QUESTION 193

- (Exam Topic 2)

What are the four cloud deployment models? Response:

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

Answer: D

NEW QUESTION 197

- (Exam Topic 2)

The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “using components with known vulnerabilities.”

Why would an organization ever use components with known vulnerabilities to create software? Response:

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

Answer: B

NEW QUESTION 199

- (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)

What is a form of cloud storage where data is stored as objects, arranged in a hierarchal structure, like a file tree?

Response:

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

Answer: D

NEW QUESTION 207

- (Exam Topic 2)

Each of the following is an element of the Identification phase of the identity and access management (IAM) process except _____.

Response:

- A. Provisioning
- B. Inversion
- C. Management
- D. Deprovisioning

Answer: B

NEW QUESTION 211

- (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 213

- (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 216

- (Exam Topic 2) What are SOCI/SOCII/SOCIII? Response:

- A. Risk management frameworks
- B. Access controls
- C. Audit reports
- D. Software development phases

Answer: C

NEW QUESTION 220

- (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 224

- (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 228

- (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 233

- (Exam Topic 2)

Federation should be _____ to the users.

Response:

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

Answer: C

NEW QUESTION 235

- (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 237

- (Exam Topic 2)

Which type of testing tends to produce the best and most comprehensive results for discovering system vulnerabilities?

Response:

- A. Static
- B. Dynamic
- C. Pen
- D. Vulnerability

Answer: A

NEW QUESTION 240

- (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 242

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 243

- (Exam Topic 2)

Which of the following data protection methodologies maintains the ability to connect back values to the original values?

Response:

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

Answer: A

NEW QUESTION 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 involves assigning an opaque value to sensitive data fields to protect confidentiality? Response:

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

Answer: C

NEW QUESTION 248

- (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)

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 254

- (Exam Topic 3)

Cloud vendors are held to contractual obligations with specified metrics by:

Response:

- A. SLAs
- B. Regulations
- C. Law
- D. Discipline

Answer: A

NEW QUESTION 259

- (Exam Topic 3)

Which technology is most associated with tunneling? Response:

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

Answer: B

NEW QUESTION 260

- (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 264

- (Exam Topic 3)

Although indirect identifiers cannot alone point to an individual, the more of them known can lead to a specific identity. Which strategy can be used to avoid such a connection being made?

Response:

- A. Masking
- B. Anonymization
- C. Obfuscation
- D. Encryption

Answer: B

NEW QUESTION 268

- (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 269

- (Exam Topic 3)

When a customer performs a penetration test in the cloud, why isn't the test an optimum simulation 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 271

- (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 273

- (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 274

- (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 279

- (Exam Topic 3)

Cryptographic keys for encrypted data stored in the cloud should be _____.

Response:

- A. At least 128 bits long
- B. Not stored with the cloud provider
- C. Split into groups
- D. Generated with redundancy

Answer: B

NEW QUESTION 281

- (Exam Topic 3)

You are developing a new process for data discovery for your organization and are charged with ensuring that all applicable data is included. Which of the following is NOT one of the three methods of data discovery?

Response:

- A. Metadata
- B. Content analysis
- C. Labels
- D. Classification

Answer: D

NEW QUESTION 283

- (Exam Topic 3)

Which of the following is an example of useful and sufficient data masking of the string "CCSP"? Response:

- A. XCSP
- B. PSCC
- C. TtLp
- D. 3X91

Answer: C

NEW QUESTION 288

- (Exam Topic 3)

Which of the following aids in the ability to demonstrate due diligence efforts?

Response:

- A. Redundant power lines
- B. HVAC placement
- C. Security training documentation
- D. Bollards

Answer: C

NEW QUESTION 289

- (Exam Topic 3)

The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. A cloud customer that does not perform sufficient due diligence can suffer harm if the cloud provider they've selected goes out of business.

What do we call this problem? Response:

- A. Vendor lock-in
- B. Vendor lock-out
- C. Vendor incapacity
- D. Unscaled

Answer: B

NEW QUESTION 292

- (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 295

- (Exam Topic 3)

When using an Infrastructure as a Service (IaaS) solution, what is the capability provided to the customer? Response:

- A. To provision processing, storage, networks, and other fundamental computing resources when the consumer is not able to deploy and run arbitrary software, which can include operating systems and applications.
- B. To provision processing, storage, networks, and other fundamental computing resources when the provider is able to deploy and run arbitrary software, which can include operating systems and applications.
- C. To provision processing, storage, networks, and other fundamental computing resources when the auditor is able to deploy and run arbitrary software, which

can include operating systems and applications.

D. To provision processing, storage, networks, and other fundamental computing resources when the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Answer: D

NEW QUESTION 296

- (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 301

- (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 303

- (Exam Topic 3)

What type of identity system allows trust and verifications between the authentication systems of multiple organizations?

Response:

- A. Federated
- B. Collaborative
- C. Integrated
- D. Bidirectional

Answer: A

NEW QUESTION 306

- (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 307

- (Exam Topic 3)

When a user accesses a system, what process determines the roles and privileges that user is granted within the application?

Response:

- A. Authorization
- B. Authentication
- C. Provisioning
- D. Privilege

Answer: A

NEW QUESTION 310

- (Exam Topic 3)

What are the objectives of change management? (Choose all that apply.)

Response:

- A. Respond to a customer's changing business requirements while maximizing value and reducing incidents, disruption, and rework
- B. Ensure that changes are recorded and evaluated
- C. Respond to business and IT requests for change that will disassociate services with business needs
- D. Ensure that all changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner

Answer: AB

NEW QUESTION 313

- (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 315

- (Exam Topic 3)

Which is the most commonly used standard for information exchange within a federated identity system? Response:

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

Answer: C

NEW QUESTION 318

- (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 320

- (Exam Topic 3)

In addition to BCDR, what other benefit can your data archive/backup provide? Response:

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

Answer: D

NEW QUESTION 324

- (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 325

- (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 329

- (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 334

- (Exam Topic 3)

Your application has been a continued target for SQL injection attempts. Which of the following technologies would be best used to combat the likeliness of a successful SQL injection exploit from occurring?

Response:

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

Answer: B

NEW QUESTION 338

- (Exam Topic 3)

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

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * CCSP Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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