



ISC2

Exam Questions CCSP

Certified Cloud Security Professional

NEW QUESTION 1

A virtual network interface card (NIC) exists at layer _____ of the OSI model. Response:

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

Answer: A

NEW QUESTION 2

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

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

Answer: C

NEW QUESTION 3

You are the security manager for a small application development company. Your company is considering the use of the cloud for software testing purposes. Which cloud service model is most likely to suit your needs?

Response:

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

Answer: B

NEW QUESTION 4

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 5

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 6

All of the following are usually nonfunctional requirements except _____.

Response:

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

Answer: D

NEW QUESTION 7

Which of the following is characterized by a set maximum capacity? Response:

- A. A secret-sharing-made-short (SSMS) bit-splitting implementation
- B. A tightly coupled cloud storage cluster
- C. A loosely coupled cloud storage cluster
- D. A public-key infrastructure

Answer: B

NEW QUESTION 8

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 9

What type of device is often leveraged to assist legacy applications that may not have the programmatic capability to process assertions from modern web services?

- A. Web application firewall
- B. XML accelerator
- C. Relying party
- D. XML firewall

Answer: B

NEW QUESTION 10

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 10

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 14

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

Which of the following is a good way to protect against this problem? Response:

- A. Don't use redirects/forwards in your applications.
- B. Refrain from storing credentials long term.
- C. Implement security incident/event monitoring (security information and event management (SIEM)/security information management (SIM)/security event management (SEM)) solutions.
- D. Implement digital rights management (DRM) solutions.

Answer: A

NEW QUESTION 19

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 23

Which concept of cloud computing pertains to the ability to reuse components and services of an application for other purposes?

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

Answer: B

NEW QUESTION 25

You have been tasked with creating an audit scope statement and are making your project outline. Which of the following is NOT typically included in an audit scope statement?

- A. Statement of purpose
- B. Deliverables
- C. Classification
- D. Costs

Answer: D

NEW QUESTION 29

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

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

Answer: B

NEW QUESTION 30

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 33

Of the following, which is probably the most significant risk in a managed cloud environment? Response:

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

Answer: B

NEW QUESTION 36

Which document will enforce uptime and availability requirements between the cloud customer and cloud provider? Response:

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

Answer: C

NEW QUESTION 39

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 44

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 46

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 51

Which of the following are contractual components that the CSP should review and understand fully when contracting with a cloud service provider? (Choose two.)

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

Answer: BD

NEW QUESTION 56

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 57

The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet). In a typical TLS session, who initiates the protocol?

Response:

- A. The server
- B. The client
- C. The certifying authority
- D. The ISP

Answer: B

NEW QUESTION 60

_____ 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 63

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 67

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 71

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 75

Which of the following is the best and only completely secure method of data destruction? Response:

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

Answer: C

NEW QUESTION 78

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 82

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 87

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 92

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 93

Who is ultimately responsible for a data breach that includes personally identifiable information (PII), in the event of negligence on the part of the cloud provider?

- A. The user

- B. The subject
- C. The cloud provider
- D. The cloud customer

Answer: D

NEW QUESTION 94

Which of the following is not one of the defined security controls domains within the Cloud Controls Matrix, published by the Cloud Security Alliance?
Response:

- A. Financial
- B. Human resources
- C. Mobile security
- D. Identity and access management

Answer: A

NEW QUESTION 98

Different types of cloud deployment models use different types of storage from traditional data centers, along with many new types of software platforms for deploying applications and configurations. Which of the following is NOT a storage type used within a cloud environment?

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

Answer: A

NEW QUESTION 102

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 103

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 107

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 110

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 115

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 118

The final phase of the cloud data lifecycle is the destroy phase, where data is ultimately deleted and done so in a secure manner to ensure it cannot be recovered or reconstructed. Which cloud service category poses the most challenges to data destruction or the cloud customer?

- A. Platform
- B. Software
- C. Infrastructure
- D. Desktop

Answer: B

NEW QUESTION 121

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 125

Which of the following data sanitation methods would be the MOST effective if you needed to securely remove data as quickly as possible in a cloud environment? Response:

- A. Zeroing
- B. Cryptographic erasure
- C. Overwriting
- D. Degaussing

Answer: B

NEW QUESTION 127

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 132

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 136

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. Management is interested in adopting an Agile development style.

This will be typified by which of the following traits? Response:

- A. Reliance on a concrete plan formulated during the Define phase
- B. Rigorous, repeated security testing
- C. Isolated programming experts for specific functional elements
- D. Short, iterative work periods

Answer: D

NEW QUESTION 138

When a data center is configured such that the backs of the devices face each other and the ambient temperature in the work area is cool, it is called _____.
Response:

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

Answer: A

NEW QUESTION 143

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 148

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 151

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 152

All of the following are terms used to describe 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 156

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 159

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 160

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 162

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 165

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 166

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

According to the CSA, an organization that suffers a data breach might suffer all of the following negative effects except _____.

Response:

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

Answer: D

NEW QUESTION 169

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 170

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 174

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 175

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 177

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 179

Which of the following is not an enforceable governmental request? Response:

- A. Warrant
- B. Subpoena
- C. Court order
- D. Affidavit

Answer: D

NEW QUESTION 180

Who is the entity identified by personal data? Response:

- A. The data owner
- B. The data processor
- C. The data custodian
- D. The data subject

Answer: D

NEW QUESTION 183

DRM solutions should generally include all the following functions, except:

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

Answer: B

NEW QUESTION 187

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 191

SOX was enacted because of which of the following? Response:

- A. Poor BOD oversight
- B. Lack of independent audits
- C. Poor financial controls
- D. All of the above

Answer: D

NEW QUESTION 196

A honeypot should contain data_____.
Response:

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

Answer: C

NEW QUESTION 198

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 199

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 201

Which standards body depends heavily on contributions and input from its open membership base? Response:

- A. NIST
- B. ISO
- C. ICANN
- D. CSA

Answer: D

NEW QUESTION 206

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 209

_____ is the most prevalent protocol used in identity federation.

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

Answer: B

NEW QUESTION 212

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 217

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 218

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 219

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 222

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 225

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 228

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 229

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 233

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 234

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 237

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 240

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

According to the CSA, what aspect of managed cloud services makes the threat of malicious insiders so alarming?

Response:

- A. Scalability
- B. Multitenancy
- C. Metered service
- D. Flexibility

Answer: B

NEW QUESTION 241

Which key storage solution would be the BEST choice in a situation where availability might be of a particular concern?

Response:

- A. Internal
- B. External
- C. Hosted
- D. Embedded

Answer: A

NEW QUESTION 242

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 243

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 247

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 252

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 253

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 254

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 259

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 261

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 266

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 268

Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likelihood 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 273

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 277

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 281

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 285

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 290

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 293

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 298

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 301

An organization could have many reasons that are common throughout the industry to activate a BCDR situation. Which of the following is NOT a typical reason to activate a BCDR plan?

Response:

- A. Natural disaster
- B. Utility outage
- C. Staff loss
- D. Terrorist attack

Answer: C

NEW QUESTION 304

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 305

Which of the following would NOT be included as input into the requirements gathering for an application or system?

Response:

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

Answer: D

NEW QUESTION 310

Resolving resource contentions in the cloud will most likely be the job of the _____.

Response:

- A. Router
- B. Emulator
- C. Regulator
- D. Hypervisor

Answer: D

NEW QUESTION 311

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 312

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 315

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 319

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 322

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 324

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 325

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 matter
- E. Data can be saved anywhere without consequence

Answer: A

NEW QUESTION 328

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 332

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 336

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 339

Which of the following is the correct name for Tier II of the Uptime Institute Data Center Site Infrastructure Tier Standard Topology?
Response:

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

Answer: D

NEW QUESTION 344

Tokenization requires at least _____ database(s).
Response:

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

Answer: B

NEW QUESTION 349

There are two general types of smoke detectors. Which type uses a small portion of radioactive material? Response:

- A. Photoelectric
- B. Ionization
- C. Electron pulse
- D. Integral field

Answer: B

NEW QUESTION 352

Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?
Response:

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

Answer: C

NEW QUESTION 355

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 356

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 360

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 361

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 364

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 367

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 369

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 373

Halon is now illegal to use for data center fire suppression. What is the reason it was outlawed? Response:

- A. It poses a threat to health and human safety when deployed.
- B. It can harm the environment.
- C. It does not adequately suppress fires.
- D. It causes undue damage to electronic systems.

Answer: B

NEW QUESTION 377

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 381

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 383

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 384

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 388

What aspect of data center planning occurs first? Response:

- A. Logical design
- B. Physical design
- C. Audit
- D. Policy revision

Answer: B

NEW QUESTION 390

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 392

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 396

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 401

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 403

All of the following might be used as data discovery characteristics in a content-analysis-based data discovery effort except _____.
Response:

- A. Keywords
- B. Pattern-matching
- C. Frequency
- D. Inheritance

Answer: D

NEW QUESTION 407

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 412

Federation should be _____ to the users.
Response:

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

Answer: C

NEW QUESTION 417

The Restatement (Second) Conflict of Law refers to which of the following? Response:

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

Answer: A

NEW QUESTION 421

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 422

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 425

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 429

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 433

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 434

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 435

You have been tasked by management to offload processing and validation of incoming encoded data from your application servers and their associated APIs. Which of the following would be the most appropriate device or software to consider?
Response:

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

Answer: A

NEW QUESTION 438

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 441

You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization.

What is probably the best benefit offered by the CCM? Response:

- A. The low cost of the tool
- B. Allowing your organization to leverage existing controls across multiple frameworks so as not to duplicate effort
- C. Simplicity of control selection from the list of approved choices
- D. Ease of implementation by choosing controls from the list of qualified vendors

Answer: B

NEW QUESTION 446

DLP solutions typically involve all of the following aspects except _____.

Response:

- A. Data discovery
- B. Tokenization
- C. Monitoring
- D. Enforcement

Answer: B

NEW QUESTION 448

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

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

Answer: C

NEW QUESTION 453

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 454

An audit against the _____ will demonstrate that an organization has inadequate security controls to meet its ISO 27001 requirements.

Response:

- A. SAS 70 standard
- B. SSAE 16 standard
- C. ISO 27002 certification criteria
- D. NIST SP 800-53

Answer: C

NEW QUESTION 459

Your organization is developing software for wide use by the public. You have decided to test it in a cloud environment, in a PaaS model. Which of the following should be of particular concern to your organization for this situation?

Response:

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

Answer: B

NEW QUESTION 463

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 467

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 472

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 473

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 478

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 483

Which of the following is not a way to manage risk? Response:

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

Answer: A

NEW QUESTION 488

The tasks performed by the hypervisor in the virtual environment can most be likened to the tasks of the _____ in the legacy environment.

Response:

- A. Central processing unit (CPU)
- B. Security team
- C. OS
- D. PGP

Answer: A

NEW QUESTION 493

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 498

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 501

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 502

Federation allows _____ across organizations.

Response:

- A. Role replication
- B. Encryption
- C. Policy
- D. Access

Answer: D

NEW QUESTION 506

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

Response:

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

Answer: A

NEW QUESTION 507

A user signs on to a cloud-based social media platform. In another browser tab, the user finds an article worth posting to the social media platform. The user clicks on the platform's icon listed on the article's website, and the article is automatically posted to the user's account on the social media platform.

This is an example of what?

Response:

- A. Single sign-on
- B. Insecure direct identifiers
- C. Identity federation
- D. Cross-site scripting

Answer: C

NEW QUESTION 512

Which kind of SSAE report comes with a seal of approval from a certified auditor? Response:

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

Answer: C

NEW QUESTION 516

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 518

Which of the following methods for the safe disposal of electronic records can always be used in a cloud environment? Response:

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

Answer: B

NEW QUESTION 521

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 522

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 527

Digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM) often protect unauthorized distribution of what type of intellectual property?
Response:

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

Answer: D

NEW QUESTION 529

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 533

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 535

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 540

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 542

A cloud provider is looking to provide a higher level of assurance to current and potential cloud customers about the design and effectiveness of their security controls.

Which of the following audit reports would the cloud provider choose as the most appropriate to accomplish this goal?

Response:

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

Answer: D

NEW QUESTION 547

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 552

Digital rights management (DRM) tools can be combined with _____, to enhance security capabilities. Response:

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

Answer: B

NEW QUESTION 554

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 559

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 564

Which of the following is not a component of the STRIDE model? Response:

- A. Spoofing
- B. Repudiation

- C. Information disclosure
- D. External pen testing

Answer: D

NEW QUESTION 566

The ISO/IEC 27001:2013 security standard contains 14 different domains that cover virtually all areas of IT operations and procedures. Which of the following is NOT one of the domains listed in the standard?

Response:

- A. Legal
- B. Management
- C. Assets
- D. Supplier Relationships

Answer: A

NEW QUESTION 569

Which type of cloud-based storage is IRM typically associated with? Response:

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

Answer: D

NEW QUESTION 574

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 576

Proper _____ need to be assigned to each data classification/category. Response:

- A. Dollar values
- B. Metadata
- C. Security controls
- D. Policies

Answer: C

NEW QUESTION 580

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 581

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 583

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 587

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 589

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 594

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 599

DLP solutions can aid all of the following security-related efforts except _____.

Response:

- A. Access control
- B. Egress monitoring
- C. e-discovery/forensics
- D. Data categorization/classification

Answer: A

NEW QUESTION 602

With data in transit, which of the following will be the MOST major concern in order for a DLP solution to properly work?

Response:

- A. Scalability
- B. Encryption
- C. Redundancy
- D. Integrity

Answer: B

NEW QUESTION 605

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 608

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 610

FM-200 has all the following properties except _____.

Response:

- A. It's nontoxic at levels used for fire suppression
- B. It's gaseous at room temperature
- C. It may deplete the Earth's ozone layer
- D. It does not leave a film or coagulant after use

Answer: C

NEW QUESTION 612

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 614

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 616

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 620

All of these are reasons an organization may want to consider cloud migration except: Response:

- A. Reduced personnel costs
- B. Elimination of risks
- C. Reduced operational expenses
- D. Increased efficiency

Answer: B

NEW QUESTION 624

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 629

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 631

Which of the following is not included in the OWASP Top Ten web application security threats? Response:

- A. Injection
- B. Cross-site scripting
- C. Internal theft
- D. Sensitive data exposure

Answer: C

NEW QUESTION 633

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 634

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 635

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 637

Which of the following methods of addressing risk is most associated with insurance? Response:

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

Answer: A

NEW QUESTION 640

Tokenization requires two distinct _____.
Response:

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

D. Personnel

Answer: B

NEW QUESTION 641

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 643

Your company operates in a highly competitive market, with extremely high-value data assets. Senior management wants to migrate to a cloud environment but is concerned that providers will not meet the company's security needs.

Which deployment model would probably best suit the company's needs? Response:

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

Answer: B

NEW QUESTION 647

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 650

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 654

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 657

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 659

Who operates the management plane? Response:

- A. Regulators
- B. End consumers
- C. Privileged users
- D. Privacy data subjects

Answer: C

NEW QUESTION 661

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 663

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 666

You are the security manager for a small surgical center. Your organization is reviewing upgrade options for its current, on-premises data center. In order to best meet your needs, which one of the following options would you recommend to senior management?

Response:

- A. Building a completely new data center
- B. Leasing a data center that is currently owned by another firm
- C. Renting private cloud space in a Tier 2 data center
- D. Staying with the current data center

Answer: A

NEW QUESTION 670

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 671

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 674

In which of the following situations does the data owner have to administer the OS? Response:

- A. IaaS
- B. PaaS
- C. Offsite archive
- D. SaaS

Answer: A

NEW QUESTION 675

Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?

Response:

- A. SOC 1
- B. SOC 2

- C. SOC 3
- D. SOC 4

Answer: B

NEW QUESTION 676

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 680

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 683

Managed cloud services exist because the service is less expensive for each customer than creating the same services for themselves in a legacy environment. Using a managed service allows the customer to realize significant cost savings through the reduction of _____.

Response:

- A. Risk
- B. Security controls
- C. Personnel
- D. Data

Answer: C

NEW QUESTION 684

The BIA can be used to provide information about all the following, except: Response:

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

Answer: B

NEW QUESTION 689

In general, a cloud BCDR solution will be _____ than a physical solution. Response:

- A. Slower
- B. Less expensive
- C. Larger
- D. More difficult to engineer

Answer: B

NEW QUESTION 693

What is one of the benefits of implementing an egress monitoring solution? Response:

- A. Preventing DDoS attacks
- B. Inventorying data assets
- C. Interviewing data owners
- D. Protecting against natural disasters

Answer: B

NEW QUESTION 698

Software-defined networking (SDN) is intended to separate different network capabilities and allow for the granting of granular configurations, permissions, and features to non-network staff or customers. Which network capability is separated from forwarding of traffic?

Response:

- A. Routing
- B. Firewalling
- C. Filtering
- D. IPS

Answer: C

NEW QUESTION 699

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 703

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 705

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 710

.....

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](#)