
# ISC2

## Exam Questions CCSP

Certified Cloud Security Professional

**NEW QUESTION 1**
Under EU law, a cloud customer who gives sensitive data to a cloud provider is still legally responsible for the damages resulting from a data breach caused by the provider; the EU would say that it is the cloud customer's fault for choosing the wrong provider.
This is an example of insufficient _____ .

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

**Answer:** C

**NEW QUESTION 2**
_____ can often be the result of inadvertent activity. Response:

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

**Answer:** C

**NEW QUESTION 3**
What can tokenization be used for? Response:

A. Encryption
B. Compliance with PCI DSS
C. Enhancing the user experience
D. Giving management oversight to e-commerce functions

**Answer:** B

**NEW QUESTION 4**
DLP can be combined with what other security technology to enhance data controls? Response:

A. DRM
B. SIEM
C. Kerberos
D. Hypervisors

**Answer:** A

**NEW QUESTION 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**
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 10**
Which of the following is a risk in the cloud environment that is not existing or is as prevalent in the legacy environment?
Response:

A. Legal liability in multiple jurisdictions
B. Loss of productivity due to DDoS
C. Ability of users to gain access to their physical workplace
D. Fire

**Answer:** A

**NEW QUESTION 12**
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 16**
What is the federal agency that accepts applications for new patents?

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

**Answer:** B

**NEW QUESTION 21**
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 25**
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 30**
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 34**
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 39**
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 41**
A typical DLP tool can enhance the organization's efforts at accomplishing what legal task? Response:

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

**Answer:** A

**NEW QUESTION 45**
Which of the following is not a factor an organization might use in the cost-benefit analysis when deciding whether to migrate to a cloud environment?
Response:

A. Pooled resources in the cloud
B. Shifting from capital expenditures to support IT investment to operational expenditures
C. The time savings and efficiencies offered by the cloud service
D. Branding associated with which cloud provider might be selected

**Answer:** D

**NEW QUESTION 49**
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 51**
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 56**
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 57**
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 58**
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 61**
Which of the following tools might be useful in data discovery efforts that are based on content analysis?

A. DLP
B. Digital Rights Management (DRM)
C. iSCSI
D. Fibre Channel over Ethernet (FCoE)

**Answer:** A

**NEW QUESTION 64**
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 65**
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 69**
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
What should you not expect the tool to address? Response:

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

**Answer:** B

**NEW QUESTION 72**
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 73**
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 75**
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 79**
Which of the following storage types are used with an Infrastructure as a Service (IaaS) solution? Response:

A. Volume and block
B. Structured and object
C. Unstructured and ephemeral
D. Volume and object

**Answer:** D

**NEW QUESTION 81**
What sort of legal enforcement may the Payment Card Industry (PCI) Security Standards Council not bring to bear against organizations that fail to comply with the Payment Card Industry Data Security Standard (PCI DSS)?
Response:

A. Fines
B. Jail time
C. Suspension of credit card processing privileges
D. Subject to increased audit frequency and scope

**Answer:** B

**NEW QUESTION 82**
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 86**
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 89**
Which of the following is a possible negative aspect of bit-splitting?

A. Greater chance of physical theft of assets
B. Loss of public image
C. Some risk to availability, depending on the implementation
D. A small fire hazard

**Answer:** C

**NEW QUESTION 94**
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 99**
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 102**
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 104**
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 108**
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 109**
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 114**
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 119**
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 120**
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 124**
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 127**
Which security certification serves as a general framework that can be applied to any type of system or application?

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

**Answer:** A

**NEW QUESTION 131**
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 135**
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:
Response:

A. Tokenization
B. Data discovery
C. Obfuscation
D. Masking

**Answer:** B

**NEW QUESTION 138**
Which of the following top security threats involves attempting to send invalid commands to an application in an attempt to get the application to execute the code?
Response:

A. Cross-site scripting
B. Injection
C. Insecure direct object references
D. Cross-site request forgery

**Answer:** B

**NEW QUESTION 139**
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “sensitive data exposure.” Which of these is a technique to reduce the potential for a sensitive data exposure? Response:

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

**Answer:** A

**NEW QUESTION 144**
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 145**
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 150**
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 151**
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 153**
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 157**
Data labels could include all the following, except: Response:

A. Source
B. Delivery vendor
C. Handling restrictions
D. Jurisdiction

**Answer:** B

**NEW QUESTION 161**
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 166**
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 168**
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 169**
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 171**
You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Previous releases have shipped with major flaws that were not detected in the testing phase; leadership wants to avoid repeating that problem. What tool/technique/technology might you suggest to aid in identifying programming errors?

A. Vulnerability scans

B. Open source review
C. SOC audits
D. Regulatory review

**Answer:** B

**NEW QUESTION 176**
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 181**
Who should be the only entity allowed to declare that an organization can return to normal following contingency or BCDR operations?
Response:

A. Regulators
B. Law enforcement
C. The incident manager
D. Senior management

**Answer:** D

**NEW QUESTION 186**
Which of the following management risks can make an organization's cloud environment unviable? Response:

A. Insider trading
B. VM sprawl
C. Hostile takeover
D. Improper personnel selection

**Answer:** B

**NEW QUESTION 187**
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 190**
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 193**
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
In order to increase the security value of the DLP, you should consider combining it with _____.
Response:

A. Digital rights management (DRM) and security event and incident management (SIEM) tools
B. An investment in upgraded project management software
C. Digital insurance policies
D. The Uptime Institute's Tier certification

**Answer:** A

**NEW QUESTION 194**
The Cloud Security Alliance (CSA) publishes, the Notorious Nine, a list of common threats to organizations participating in cloud computing.
According to the CSA, all of the following activity can result in data loss except _____ .

A. Misplaced crypto keys
B. Improper policy

C. Ineffectual backup procedures
D. Accidental overwrite

**Answer:** B

**NEW QUESTION 197**
Heating, ventilation, and air conditioning (HVAC) systems cool the data center by pushing warm air into _____.
Response:

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

**Answer:** D

**NEW QUESTION 201**
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 205**
At which layer does the IPSec protocol operate to encrypt and protect communications between two parties? Response:

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

**Answer:** A

**NEW QUESTION 208**
_____ is the most prevalent protocol used in identity federation.

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

**Answer:** B

**NEW QUESTION 212**
When using transparent encryption of a database, where does the encryption engine reside? Response:

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

**Answer:** D

**NEW QUESTION 215**
What are the six components that make up the STRIDE threat model? Response:

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

**Answer:** A

**NEW QUESTION 216**
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 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 220**
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 225**
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**
Penetration testing is a(n) _____ form of security assessment.
Response:

A. Active
B. Comprehensive
C. Total
D. Inexpensive

**Answer:** A

**NEW QUESTION 232**
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**
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 239**
A bare-metal hypervisor is Type _____.
Response:

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

**Answer:** A

**NEW QUESTION 244**
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 246**
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 251**
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 252**
The destruction of a cloud customer's data can be required by all of the following except _____.
Response:

A. Statute
B. Regulation
C. The cloud provider's policy
D. Contract

**Answer:** C

**NEW QUESTION 255**
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 258**
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 259**
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 261**
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 262**
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**
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 270**
Which of the following is not one of the types of controls? Response:

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

**Answer:** A

**NEW QUESTION 272**
Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?
Response:

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

**Answer:** A

**NEW QUESTION 275**
Which of the following is NOT a core component of an SIEM solution? Response:

A. Correlation
B. Aggregation
C. Compliance
D. Escalation

**Answer:** D

**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 280**
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 284**
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 289**
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 293**
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 295**
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 298**
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 301**
All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline except _____.
Response:

A. Remove all nonessential programs from the baseline image
B. Exclude the target system you intend to baseline from any scheduled updates/patching used inproduction systems
C. Include the baseline image in the asset inventory/configuration management database
D. Configure the host OS according to the baseline requirements

**Answer:** C

**NEW QUESTION 305**
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 309**
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 314**
Why does the physical location of your data backup and/or BCDR failover environment matter? Response:

A. It may affect regulatory compliance
B. Lack of physical security
C. Environmental factors such as humidity
D. It doesn’t matte
E. Data can be saved anywhere without consequence

**Answer:** A

**NEW QUESTION 316**
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 319**
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 320**
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 322**
Tokenization requires at least _____ database(s).
Response:

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

**Answer:** B

**NEW QUESTION 323**
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 325**
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 329**
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 330**
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 333**
All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline, except _____.
Response:

A. Audit the baseline to ensure that all configuration items have been included and applied correctly
B. Impose the baseline throughout the environment
C. Capture an image of the baseline system for future reference/versioning/rollback purposes
D. Document all baseline configuration elements and versioning data

**Answer:** B

**NEW QUESTION 334**
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 335**
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 340**
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 343**
Data transformation in a cloud environment should be of great concern to organizations considering cloud migration because _____ could affect data classification processes/implementations.
Response:

A. Multitenancy
B. Virtualization
C. Remote access
D. Physical distance

**Answer:** B

**NEW QUESTION 347**
What is a cloud storage architecture that manages the data in a hierarchy of files? Response:

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

**Answer:** B

**NEW QUESTION 349**
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 350**
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 353**
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 354**
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 359**
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 363**
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 364**
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 368**
What aspect of data center planning occurs first? Response:

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

**Answer:** B

**NEW QUESTION 369**
TLS provides _____ and _____ for communications. Response:

A. Privacy, security
B. Security, optimization
C. Privacy, integrity
D. Enhancement, privacy

**Answer:** C

**NEW QUESTION 374**
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 379**
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 384**
You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center.
One of the challenges you're facing is whether the provider will have undue control over your data once it is within the provider's data center; will the provider be able to hold your organization hostage because they have your data?
This is a(n) _____ issue. Response:

A. Interoperability
B. Portability
C. Availability
D. Security

**Answer:** B

**NEW QUESTION 387**
Federation should be _____ to the users.
Response:

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

**Answer:** C

**NEW QUESTION 390**
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 393**
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 395**
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 396**
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 399**
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 400**
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 404**
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 405**
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 409**
DLP solutions typically involve all of the following aspects except _____.
Response:

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

**Answer:** B

**NEW QUESTION 413**
Which of the following is a method for apportioning resources that involves prioritizing resource requests to resolve contention situations?
Response:

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

**Answer:** B

**NEW QUESTION 416**
_____ can often be the result of inadvertent activity. Response:

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

**Answer:** C

**NEW QUESTION 421**
An audit against the _____ will demonstrate that an organization has ¬adequate 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 424**
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 425**
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 430**
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 434**
You are the IT director for a small contracting firm. Your company is considering migrating to a cloud production environment.
Which service model would best fit your needs if you wanted an option that reduced the chance of vendor lock-in but also did not require the highest degree of administration by your own personnel?
Response:

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

**Answer:** B

**NEW QUESTION 437**
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 442**
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 444**
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 447**
Which of the following is not a way to manage risk? Response:

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

**Answer:** A

**NEW QUESTION 449**
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 450**
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 455**
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 458**
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 463**
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 468**
Federation allows _____ across organizations.
Response:

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

**Answer:** D

**NEW QUESTION 472**
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 476**
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 480**
In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?
Response:

A. Technological
B. Physical
C. Administrative
D. All of the above

**Answer:** D

**NEW QUESTION 482**
Which technology is most associated with tunneling? Response:

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

**Answer:** B

**NEW QUESTION 485**
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 490**
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 494**
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 499**
Devices in the cloud datacenter should be secure against attack. All the following are means of hardening devices, except:
Response:

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

**Answer:** D

**NEW QUESTION 503**
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 504**
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 509**
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 512**
What is the main reason virtualization is used in the cloud? Response:

A. VMs are easier to administer
B. If a VM is infected with malware, it can be easily replaced
C. With VMs, the cloud provider does not have to deploy an entire hardware device for every new user
D. VMs are easier to operate than actual devices

**Answer:** C

**NEW QUESTION 513**
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 518**
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 520**
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 525**
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 527**
Which type of cloud-based storage is IRM typically associated with? Response:

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

**Answer:** D

**NEW QUESTION 531**
Which of the following data-sanitation approaches are always available within a cloud environment? Response:

A. Physical destruction
B. Shredding
C. Overwriting
D. Cryptographic erasure

**Answer:** D

**NEW QUESTION 535**
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 537**
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 540**
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “security misconfiguration.” Which of these is a technique to reduce the potential for a security misconfiguration? Response:

A. Get regulatory approval for major configuration modifications.
B. Update the BCDR plan on a timely basis.
C. Train all users on proper security procedures.
D. Perform periodic scans and audits of the environment.

**Answer:** D

**NEW QUESTION 544**
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 548**
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 553**
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 556**
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 557**
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 561**
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 565**
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 568**
What is the cloud service model in which the customer is responsible for administration of the OS? Response:

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

**Answer:** A

**NEW QUESTION 571**
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 575**
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 576**
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 581**
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 584**
Which theoretical technology would allow superposition of physical states to increase both computing capacity and encryption keyspace?
Response:

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

**Answer:** B

**NEW QUESTION 587**
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 589**
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 591**
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 592**
Virtual machine (VM) configuration management (CM) tools should probably include _____.
Response:

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

**Answer:** C

**NEW QUESTION 593**
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 594**
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 595**
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 598**
Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like: Response:

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

**Answer:** C

**NEW QUESTION 601**
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 606**
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 610**
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 612**
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 617**
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 622**
Which of the following is a risk that stems from a virtualized environment? Response:

A. Live virtual machines in the production environment are moved from one host to another in the clear.
B. Cloud data centers can become a single point of failure.
C. It is difficult to find and contract with multiple utility providers of the same type (electric, water, etc.).
D. Modern SLA demands are stringent and very hard to meet.

**Answer:** A

**NEW QUESTION 625**
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 626**
Who operates the management plane? Response:

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

**Answer:** C

**NEW QUESTION 628**
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 630**
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 631**
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 635**
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 638**
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 639**
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 641**
_____ is perhaps the main external factor driving IAM efforts. Response:

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

**Answer:** A

**NEW QUESTION 644**
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 647**
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 648**
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 649**
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 652**
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 657**
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 658**
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 661**
It is important to include _____ in the design of underfloor plenums if they are also used for wiring. Response:

A. Mantraps
B. Sequestered channels
C. Heat sinks
D. Tight gaskets

**Answer:** D

**NEW QUESTION 665**
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 669**
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 672**

.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons and Answers in PDF Format

## CCSP Practice Exam Features:

* CCSP Questions and Answers Updated Frequently

* CCSP Practice Questions Verified by Expert Senior Certified Staff

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

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