

# Exam Questions CCSP

Certified Cloud Security Professional

<https://www.2passeasy.com/dumps/CCSP/>



#### NEW QUESTION 1

- (Exam Topic 1)

Vulnerability scans are dependent on \_\_\_\_\_ in order to function. Response:

- A. Privileged access
- B. Vulnerability signatures
- C. Malware libraries
- D. Forensic analysis

**Answer:** B

#### NEW QUESTION 2

- (Exam Topic 1)

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 3

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 4

- (Exam Topic 1)

Which cloud storage type uses an opaque value or descriptor to categorize and organize data? Response:

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

**Answer:** D

#### NEW QUESTION 5

- (Exam Topic 1)

All of the following are usually nonfunctional requirements except \_\_\_\_\_.

Response:

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

**Answer:** D

#### NEW QUESTION 6

- (Exam Topic 1)

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 7

- (Exam Topic 1)

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

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

Response:

- A. Cloud customers and third parties are continually enhancing and modifying APIs.
- B. APIs can have automated settings.

- C. It is impossible to uninstall APIs.
- D. APIs are a form of malware.

**Answer:** A

#### NEW QUESTION 8

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 9

- (Exam Topic 1)

Which of the following should occur at each stage of the SDLC?

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

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 1)

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 11

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 16

- (Exam Topic 1)

Which of the following best describes SAML? Response:

- A. A standard for developing secure application management logistics
- B. A standard for exchanging authentication and authorization data between security domains
- C. A standard for exchanging usernames and passwords across devices
- D. A standard used for directory synchronization

**Answer:** B

#### NEW QUESTION 20

- (Exam Topic 1)

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

Response:

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

**Answer:** B

#### NEW QUESTION 24

- (Exam Topic 1)

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 27

- (Exam Topic 1)

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 32

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 36

- (Exam Topic 1)

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 40

- (Exam Topic 1)

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

Response:

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

**Answer:** D

#### NEW QUESTION 41

- (Exam Topic 1)

\_\_\_\_\_ is the legal concept whereby a cloud customer is held to a reasonable expectation for providing security of its users' and clients' privacy data in their

control.  
Response:

- A. Due care
- B. Due diligence
- C. Liability
- D. Reciprocity

**Answer:** B

#### NEW QUESTION 43

- (Exam Topic 1)

You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment. In order to get truly holistic coverage of your environment, you should be sure to include \_\_\_\_\_ as a step in the deployment process.

Response:

- A. Getting signed user agreements from all users
- B. Installation of the solution on all assets in the cloud data center
- C. Adoption of the tool in all routers between your users and the cloud provider
- D. All of your customers to install the tool

**Answer:** A

#### NEW QUESTION 45

- (Exam Topic 1)

At which phase of the SDLC process should security begin participating?

- A. Requirements gathering
- B. Requirements analysis
- C. Design
- D. Testing

**Answer:** A

#### NEW QUESTION 46

- (Exam Topic 1)

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 50

- (Exam Topic 1)

Because PaaS implementations are so often used for software development, what is one of the vulnerabilities that should always be kept in mind? Response:

- A. Malware
- B. Loss/theft of portable devices
- C. Backdoors
- D. DoS/DDoS

**Answer:** C

#### NEW QUESTION 51

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 56

- (Exam Topic 1)

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

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

D. Community

**Answer:** D

**NEW QUESTION 58**

- (Exam Topic 1)

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

Response:

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

**Answer:** A

**NEW QUESTION 59**

- (Exam Topic 1)

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

Response:

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

**Answer:** B

**NEW QUESTION 60**

- (Exam Topic 1)

Which of the following is considered an administrative control?

- A. Access control process
- B. Keystroke logging
- C. Door locks
- D. Biometric authentication

**Answer:** A

**NEW QUESTION 61**

- (Exam Topic 1)

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 66**

- (Exam Topic 1)

Which of the following practices can enhance both operational capabilities and configuration management efforts?

Response:

- A. Regular backups
- B. Constant uptime
- C. Multifactor authentication
- D. File hashes

**Answer:** D

**NEW QUESTION 70**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 74**

- (Exam Topic 1)

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 76

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 79

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 80

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 85

- (Exam Topic 1)

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

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

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

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

**Answer:** A

#### NEW QUESTION 87

- (Exam Topic 1)

DAST checks software functionality in \_\_\_\_\_. Response:

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

**Answer:** B

#### NEW QUESTION 89

- (Exam Topic 1)

You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. 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 92

- (Exam Topic 1)

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

Response:

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

**Answer:** B

#### NEW QUESTION 96

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 99

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 100

- (Exam Topic 1)

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

Response:

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

**Answer:** D

#### NEW QUESTION 102

- (Exam Topic 1)

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 103

- (Exam Topic 1)

Which of the following are considered to be the building blocks of cloud computing? Response:

- A. Data, access control, virtualization, and services
- B. Storage, networking, printing and virtualization
- C. CPU, RAM, storage and networking
- D. Data, CPU, RAM, and access control

**Answer:** C

#### NEW QUESTION 107



- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 108

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 111

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 112

- (Exam Topic 1)

Which of the following is not typically included as a basic phase of the software development life cycle?

- A. Define
- B. Design
- C. Describe
- D. Develop

**Answer:** C

#### NEW QUESTION 117

- (Exam Topic 1)

Which ISO standard refers to addressing security risks in a supply chain?

- A. ISO 27001
- B. ISO/IEC 28000:2007
- C. ISO 18799
- D. ISO 31000:2009

**Answer:** B

#### NEW QUESTION 121

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 126

- (Exam Topic 1)

What is the primary security mechanism used to protect SOAP and REST APIs? Response:

- A. Firewalls
- B. XML firewalls
- C. Encryption

D. WAFs

**Answer:** C

**NEW QUESTION 127**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 129**

- (Exam Topic 1)

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

- A. Vulnerability scans
- B. Open source review
- C. SOC audits
- D. Regulatory review

**Answer:** B

**NEW QUESTION 131**

- (Exam Topic 1)

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

Response:

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

**Answer:** B

**NEW QUESTION 136**

- (Exam Topic 1)

Application virtualization can typically be used for .

- A. Denying access to untrusted users
- B. Detecting and mitigating DDoS attacks
- C. Replacing encryption as a necessary control
- D. Running an application on an endpoint without installing it

**Answer:** D

**NEW QUESTION 138**

- (Exam Topic 1)

Which of the following best describes a cloud carrier?

- A. A person or entity responsible for making a cloud service available to consumers
- B. The intermediary who provides connectivity and transport of cloud services between cloud providers and cloud consumers
- C. The person or entity responsible for keeping cloud services running for customers
- D. The person or entity responsible for transporting data across the Internet

**Answer:** B

**NEW QUESTION 141**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 146**

- (Exam Topic 1)

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

- A. Misplaced crypto keys
- B. Improper policy
- C. Ineffectual backup procedures
- D. Accidental overwrite

**Answer:** B

#### NEW QUESTION 150

- (Exam Topic 1)

The use of which of the following technologies will NOT require the security dependency of an operating system, other than its own?

- A. Management plane
- B. Type 1 hypervisor
- C. Type 2 hypervisor
- D. Virtual machine

**Answer:** B

#### NEW QUESTION 153

- (Exam Topic 1)

At which layer does the IPSec protocol operate to encrypt and protect communications between two parties? Response:

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

**Answer:** A

#### NEW QUESTION 155

- (Exam Topic 1)

Data labels could include all the following, except: Response:

- A. Confidentiality level
- B. Distribution limitations
- C. Access restrictions
- D. Multifactor authentication

**Answer:** D

#### NEW QUESTION 158

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 163

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 165

- (Exam Topic 1)

The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet). In a typical TLS session, what is the usual means for establishing trust between the parties?

Response:

- A. Out-of-band authentication
- B. Multifactor authentication
- C. PKI certificates
- D. Preexisting knowledge of each other

**Answer:** C

#### NEW QUESTION 170

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 175

- (Exam Topic 2)

You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.  
Which of these activities should you perform before deploying the tool? Response:

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

**Answer:** A

#### NEW QUESTION 179

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 182

- (Exam Topic 2)

Penetration testing is a(n) \_\_\_\_\_ form of security assessment.  
Response:

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

**Answer:** A

#### NEW QUESTION 186

- (Exam Topic 2)

Which of the following BCDR testing methodologies is least intrusive? Response:

- A. Walk-through
- B. Simulation
- C. Tabletop
- D. Full test

**Answer:** C

#### NEW QUESTION 187

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 190

- (Exam Topic 2)

You are the data manager for a retail company; you anticipate a much higher volume of sales activity in the final quarter of each calendar year than the other quarters.  
In order to handle these increased transactions, and to accommodate the temporary sales personnel you will hire for only that time period, you consider augmenting your internal, on-premises production environment with a cloud capability for a specific duration, and will return to operating fully on-premises after the

period of increased activity.  
This is an example of \_\_\_\_\_.  
Response:

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

**Answer:** D

#### NEW QUESTION 195

- (Exam Topic 2)

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

Response:

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

**Answer:** B

#### NEW QUESTION 199

- (Exam Topic 2)

A bare-metal hypervisor is Type \_\_\_\_\_.  
Response:

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

**Answer:** A

#### NEW QUESTION 202

- (Exam Topic 2)

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 205

- (Exam Topic 2)

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 206

- (Exam Topic 2)

You are the security director for a chain of automotive repair centers across several states. Your company uses a cloud SaaS provider, for business functions that cross several of the locations of your facilities, such as: 1) ordering parts 2) logistics and inventory 3) billing, and 4) marketing.

The manager at one of your newest locations reports that there is a competing car repair company that has a logo that looks almost exactly like the one your company uses. What will most likely affect the determination of who has ownership of the logo?

Response:

- A. Whoever first used the logo
- B. The jurisdiction where both businesses are using the logo simultaneously
- C. Whoever first applied for legal protection of the logo
- D. Whichever entity has the most customers that recognize the logo

**Answer:** C

#### NEW QUESTION 209

- (Exam Topic 2)

Which cloud service category is MOST likely to use a client-side key management system? Response:

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

**Answer:** B

#### NEW QUESTION 214

- (Exam Topic 2)

The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program has \_\_\_\_\_ tiers.

Response:

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

**Answer:** B

#### NEW QUESTION 218

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 221

- (Exam Topic 2)

Although encryption can help an organization to effectively decrease the possibility of data breaches, which other type of threat can it increase the chances of?

Response:

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

**Answer:** B

#### NEW QUESTION 222

- (Exam Topic 2)

Which of the following methods is often used to obscure data from production systems for use in test or development environments?

Response:

- A. Tokenization
- B. Encryption
- C. Masking
- D. Classification

**Answer:** C

#### NEW QUESTION 227

- (Exam Topic 2)

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

Response:

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

**Answer:** A

#### NEW QUESTION 228

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 231

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 235

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 237

- (Exam Topic 2)

Who should be involved in review and maintenance of user accounts/access? Response:

- A. The user's manager
- B. The security manager
- C. The accounting department
- D. The incident response team

**Answer:** A

#### NEW QUESTION 238

- (Exam Topic 2)

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 240

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 244

- (Exam Topic 2)

You are the IT security manager for a video game software development company. Which of the following is most likely to be your primary concern on a daily basis?

Response:

- A. Health and human safety
- B. Security flaws in your products
- C. Security flaws in your organization
- D. Regulatory compliance

**Answer:** C

#### NEW QUESTION 249

- (Exam Topic 2)

A cloud data encryption situation where the cloud customer retains control of the encryption keys and the cloud provider only processes and stores the data could be considered a \_\_\_\_\_. Response:

- A. Threat



- B. Risk
- C. Hybrid cloud deployment model
- D. Case of infringing on the rights of the provider

**Answer:** C

#### NEW QUESTION 254

- (Exam Topic 2)

You are a consultant performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost \$24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant.

The fire suppression system costs \$15 million. An insurance policy that would cover the full replacement cost of the plant costs \$1 million per month.

In order to establish the true annualized loss expectancy (ALE), you would need all of the following information except \_\_\_\_\_ .

Response:

- A. The amount of revenue generated by the plant
- B. The rate at which the plant generates revenue
- C. The length of time it would take to rebuild the plant
- D. The amount of product the plant creates

**Answer:** D

#### NEW QUESTION 255

- (Exam Topic 2)

Administrative penalties for violating the General Data Protection Regulation (GDPR) can range up to \_\_\_\_\_ .

Response:

- A. US\$100,000
- B. 500,000 euros
- C. 20,000,000 euros
- D. 1,000,000 euros

**Answer:** C

#### NEW QUESTION 258

- (Exam Topic 2)

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

Response:

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

**Answer:** B

#### NEW QUESTION 263

- (Exam Topic 2)

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 268

- (Exam Topic 2)

Which of the following would probably best aid an organization in deciding whether to migrate from a legacy environment to a particular cloud provider?

Response:

- A. Rate sheets comparing a cloud provider to other cloud providers
- B. Cloud provider offers to provide engineering assistance during the migration
- C. The cost/benefit measure of closing the organization's relocation site (hot site/warm site) and using the cloud for disaster recovery instead
- D. SLA satisfaction surveys from other (current and past) cloud customers

**Answer:** D

#### NEW QUESTION 272

- (Exam Topic 2) What does nonrepudiation mean?

Response:

- A. Prohibiting certain parties from a private conversation
- B. Ensuring that a transaction is completed before saving the results

- C. Ensuring that someone cannot turn off auditing capabilities while performing a function
- D. Preventing any party that participates in a transaction from claiming that it did not

**Answer:** D

#### NEW QUESTION 275

- (Exam Topic 2)

All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline except \_\_\_\_\_.

Response:

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

**Answer:** C

#### NEW QUESTION 279

- (Exam Topic 2)

Before deploying a specific brand of virtualization toolset, it is important to configure it according to \_\_\_\_\_.

Response:

- A. Industry standards
- B. Prevailing law of that jurisdiction
- C. Vendor guidance
- D. Expert opinion

**Answer:** C

#### NEW QUESTION 280

- (Exam Topic 2)

What is the most secure form of code testing and review? Response:

- A. Open source
- B. Proprietary/internal
- C. Neither open source nor proprietary
- D. Combination of open source and proprietary

**Answer:** D

#### NEW QUESTION 285

- (Exam Topic 2)

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

Response:

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

**Answer:** B

#### NEW QUESTION 289

- (Exam Topic 2)

Tokenization requires at least \_\_\_\_\_ database(s).

Response:

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

**Answer:** B

#### NEW QUESTION 292

- (Exam Topic 2)

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 293

- (Exam Topic 2)

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 295

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 300

- (Exam Topic 2)

Which of the following is not a feature of SAST? Response:

- A. Source code review
- B. Team-building efforts
- C. "White-box" testing
- D. Highly skilled, often expensive outside consultants

**Answer:** B

#### NEW QUESTION 305

- (Exam Topic 2)

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

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

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

**Answer:** C

#### NEW QUESTION 309

- (Exam Topic 2)

Data transformation in a cloud environment should be of great concern to organizations considering cloud migration because \_\_\_\_\_ could affect data classification processes/implementations.

Response:

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

**Answer:** B

#### NEW QUESTION 310

- (Exam Topic 2)

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

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

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

**Answer:** B

#### NEW QUESTION 314

- (Exam Topic 2)

What principle must always been included with an SOC 2 report? Response:

- A. Confidentiality
- B. Security
- C. Privacy
- D. Processing integrity

**Answer:** B

#### NEW QUESTION 318

- (Exam Topic 2)

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

Response:

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

**Answer:** D

#### NEW QUESTION 319

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 324

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

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

**Answer:** C

#### NEW QUESTION 327

- (Exam Topic 2)

TLS provides \_\_\_\_\_ and \_\_\_\_\_ for communications. Response:

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

**Answer:** C

#### NEW QUESTION 328

- (Exam Topic 2)

Which phase of the cloud data lifecycle also typically entails the process of data classification? Response:

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

**Answer:** C

#### NEW QUESTION 330

- (Exam Topic 2) What is a key component of GLBA? Response:

- A. The right to be forgotten
- B. EU Data Directives
- C. The information security program
- D. The right to audit

**Answer:** C

#### NEW QUESTION 334

- (Exam Topic 2)

You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data

center.  
One of the challenges you're facing is whether the provider will have undue control over your data once it is within the provider's data center; will the provider be able to hold your organization hostage because they have your data?  
This is a(n) \_\_\_\_\_ issue. Response:

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

**Answer:** B

#### NEW QUESTION 337

- (Exam Topic 2)  
Which of the following is a possible negative aspect of bit-splitting? Response:

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

**Answer:** A

#### NEW QUESTION 338

- (Exam Topic 2)  
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 343

- (Exam Topic 2)  
Which of the following in a federated environment is responsible for consuming authentication tokens? Response:

- A. Relying party
- B. Identity provider
- C. Cloud services broker
- D. Authentication provider

**Answer:** A

#### NEW QUESTION 344

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

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

**Answer:** C

#### NEW QUESTION 347

- (Exam Topic 2)  
Which type of testing tends to produce the best and most comprehensive results for discovering system vulnerabilities? Response:

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

**Answer:** A

#### NEW QUESTION 350

- (Exam Topic 2)  
What is a data custodian responsible for? Response:

- A. The safe custody, transport, storage of the data, and implementation of business rules
- B. Data content, context, and associated business rules
- C. Logging and alerts for all data
- D. Customer access and alerts for all data

**Answer:** A

**NEW QUESTION 353**

- (Exam Topic 2)

A denial of service (DoS) attack can potentially impact all customers within a cloud environment with the continued allocation of additional resources. Which of the following can be useful for a customer to protect themselves from a DoS attack against another customer?

Response:

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

**Answer:** B

**NEW QUESTION 356**

- (Exam Topic 2)

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 360**

- (Exam Topic 2)

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

Response:

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

**Answer:** D

**NEW QUESTION 364**

- (Exam Topic 2)

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

Response:

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

**Answer:** B

**NEW QUESTION 365**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 370**

- (Exam Topic 2)

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

Response:

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

**Answer:** A

#### NEW QUESTION 372

- (Exam Topic 2)

From a security perspective, automation of configuration aids in \_\_\_\_\_.

Response:

- A. Enhancing performance
- B. Reducing potential attack vectors
- C. Increasing ease of use of the systems
- D. Reducing need for administrative personnel

**Answer:** B

#### NEW QUESTION 374

- (Exam Topic 3)

Which of the following is NOT one of the security domains presented within the Cloud Controls Matrix? Response:

- A. Financial security
- B. Mobile security
- C. Data center security
- D. Interface security

**Answer:** A

#### NEW QUESTION 378

- (Exam Topic 3)

The BCDR plan/process should be written and documented in such a way that it can be used by \_\_\_\_\_.

Response:

- A. Users
- B. Essential BCDR team members
- C. Regulators
- D. Someone with the requisite skills

**Answer:** D

#### NEW QUESTION 381

- (Exam Topic 3)

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 384

- (Exam Topic 3)

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

Response:

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

**Answer:** B

#### NEW QUESTION 385

- (Exam Topic 3)

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 390

- (Exam Topic 3)

Which network protocol is essential for allowing automation and orchestration within a cloud environment? Response:

- A. DNSSEC
- B. DHCP



- C. IPsec
- D. VLANs

**Answer:** B

#### NEW QUESTION 391

- (Exam Topic 3)

The Brewer-Nash security model is also known as which of the following? Response:

- A. MAC
- B. The Chinese Wall model
- C. Preventive measures
- D. RBAC

**Answer:** B

#### NEW QUESTION 393

- (Exam Topic 3)

Access should be based on \_\_\_\_\_.

Response:

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

**Answer:** B

#### NEW QUESTION 394

- (Exam Topic 3)

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 395

- (Exam Topic 3)

If bit-splitting is used to store data sets across multiple jurisdictions, how may this enhance security? Response:

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

**Answer:** A

#### NEW QUESTION 399

- (Exam Topic 3)

Typically, SSDs are \_\_\_\_\_.

Response:

- A. More expensive than spinning platters
- B. Larger than tape backup
- C. Heavier than tape libraries
- D. More subject to malware than legacy drives

**Answer:** A

#### NEW QUESTION 401

- (Exam Topic 3)

Fiber-optic lines are considered part of layer \_\_\_\_\_ of the OSI model. Response:

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

**Answer:** A

#### NEW QUESTION 405

- (Exam Topic 3)

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 410

- (Exam Topic 3)

When a customer performs a penetration test in the cloud, why isn't the test an optimum simulation of attack conditions?

Response:

- A. Attackers don't use remote access for cloud activity
- B. Advanced notice removes the element of surprise
- C. When cloud customers use malware, it's not the same as when attackers use malware
- D. Regulator involvement changes the attack surface

**Answer: B**

#### NEW QUESTION 413

- (Exam Topic 3)

Patches do all the following except \_\_\_\_\_.

Response:

- A. Address newly discovered vulnerabilities
- B. Solve cloud interoperability problems
- C. Add new features and capabilities to existing systems
- D. Address performance issues

**Answer: B**

#### NEW QUESTION 415

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 416

- (Exam Topic 3)

What type of redundancy can we expect to find in a datacenter of any tier?

Response:

- A. All operational components
- B. All infrastructure
- C. Emergency egress
- D. Full power capabilities

**Answer: C**

#### NEW QUESTION 417

- (Exam Topic 3)

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

Response:

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

**Answer: D**

#### NEW QUESTION 419

- (Exam Topic 3)

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 423**

- (Exam Topic 3)

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 427**

- (Exam Topic 3)

Your company maintains an on-premises data center for daily production activities but wants to use a cloud service to augment this capability during times of increased demand (cloud bursting).

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

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

**Answer:** D

**NEW QUESTION 428**

- (Exam Topic 3)

What is the major difference between authentication/authorization? Response:

- A. Code verification/code implementation
- B. Identity validation/access permission
- C. Inverse incantation/obverse instantiation
- D. User access/privileged access

**Answer:** B

**NEW QUESTION 433**

- (Exam Topic 3)

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

Response:

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

**Answer:** B

**NEW QUESTION 435**

- (Exam Topic 3)

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

In most cases, what is the method for reducing the risk of an injection attack? Response:

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

**Answer:** C

**NEW QUESTION 436**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 441**

- (Exam Topic 3)  
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 442

- (Exam Topic 3)  
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 445

- (Exam Topic 3)  
What type of identity system allows trust and verifications between the authentication systems of multiple organizations?  
Response:

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

**Answer:** A

#### NEW QUESTION 447

- (Exam Topic 3)  
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 452

- (Exam Topic 3)  
Tokenization requires two distinct \_\_\_\_\_.  
Response:

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

**Answer:** B

#### NEW QUESTION 455

- (Exam Topic 3)  
An audit against the \_\_\_\_\_ will demonstrate that an organization has a holistic, comprehensive security program.  
Response:

- A. SAS 70 standard
- B. SSAE 16 standard
- C. SOC 2, Type 2 report matrix
- D. ISO 27001 certification requirements

**Answer:** D

#### NEW QUESTION 456

- (Exam Topic 3)  
What are the objectives of change management? (Choose all that apply.)  
Response:

- A. Respond to a customer's changing business requirements while maximizing value and reducing incidents, disruption, and rework
- B. Ensure that changes are recorded and evaluated
- C. Respond to business and IT requests for change that will disassociate services with business needs

D. Ensure that all changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner

**Answer:** AB

**NEW QUESTION 461**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 463**

- (Exam Topic 3)

Which of the following types of software is a Type 2 hypervisor dependent on that a Type 1 hypervisor isn't? Response:

- A. VPN
- B. Firewall
- C. Operating system
- D. IDS

**Answer:** C

**NEW QUESTION 465**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 469**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 471**

- (Exam Topic 3)

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

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

Response:

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

**Answer:** B

**NEW QUESTION 475**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 480**

- (Exam Topic 3)

With cloud computing crossing many jurisdictional boundaries, it is a virtual certainty that conflicts will arise between differing regulations. What is the major impediment to resolving conflicts between multiple jurisdictions to form an overall policy?

Response:

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

**Answer:** D

#### NEW QUESTION 481

- (Exam Topic 3)

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 485

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 486

- (Exam Topic 3)

Which of the following is perhaps the best method for reducing the risk of a specific application not delivering the proper level of functionality and performance when it is moved from the legacy environment into the cloud?

Response:

- A. Remove the application from the organization's production environment, and replace it with something else.
- B. Negotiate and conduct a trial run in the cloud environment for that application before permanently migrating.
- C. Make sure the application is fully updated and patched according to all vendor specifications.
- D. Run the application in an emulator.

**Answer:** B

#### NEW QUESTION 490

- (Exam Topic 3)

It is important to include \_\_\_\_\_ in the design of underfloor plenums if they are also used for wiring. Response:

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

**Answer:** D

#### NEW QUESTION 495

- (Exam Topic 3)

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

Response:

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

**Answer:** A

#### NEW QUESTION 496

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CCSP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CCSP Product From:

<https://www.2passeasy.com/dumps/CCSP/>

## Money Back Guarantee

### 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