

# 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)

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

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

**Answer:** A

#### NEW QUESTION 3

- (Exam Topic 1)

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

Response:

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

**Answer:** B

#### NEW QUESTION 4

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

Response:

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

**Answer:** A

#### NEW QUESTION 8

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 10

- (Exam Topic 1)

Which of the following 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 15

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 17

- (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 22

- (Exam Topic 1)

You work for a government research facility. Your organization often shares data with other government research organizations.

You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations.

Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.

If you don't use cross-certification, what other model can you implement for this purpose? Response:

- A. Third-party identity broker
- B. Cloud reseller
- C. Intractable nuanced variance
- D. Mandatory access control (MAC)

**Answer:** A

#### NEW QUESTION 27

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 32

- (Exam Topic 1)

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 37

- (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 42

- (Exam Topic 1)

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

Response:

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

**Answer:** B

#### NEW QUESTION 43

- (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 48

- (Exam Topic 1)

Every cloud service provider that opts to join the CSA STAR program registry must complete a \_\_\_\_\_.

- A. SOC 2, Type 2 audit report
- B. Consensus Assessment Initiative Questionnaire (CAIQ)
- C. NIST 800-37 RMF audit
- D. ISO 27001 ISMS review

**Answer:** B

#### NEW QUESTION 53

- (Exam Topic 1)

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 57

- (Exam Topic 1)

Which of the following is the recommended operating range for temperature and humidity in a data center?

Response:

- A. Between 62 °F - 81 °F and 40% and 65% relative humidity
- B. Between 64 °F - 81 °F and 40% and 60% relative humidity
- C. Between 64 °F - 84 °F and 30% and 60% relative humidity
- D. Between 60 °F - 85 °F and 40% and 60% relative humidity

**Answer:** B

#### NEW QUESTION 62

- (Exam Topic 1)

Which of the following types of organizations is most likely to make use of open source software technologies?

- A. Government agencies
- B. Corporations
- C. Universities
- D. Military

**Answer:** C

#### NEW QUESTION 67

- (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 68

- (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 69

- (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 71**

- (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 74**

- (Exam Topic 1)

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 75**

- (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 80**

- (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 83**

- (Exam Topic 1)

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 86**

- (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 88**

- (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 90

- (Exam Topic 1)

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 91

- (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 93

- (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 98

- (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 101

- (Exam Topic 1)

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

Response:

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

**Answer:** D

#### NEW QUESTION 104

- (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 109

- (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 110

- (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 111

- (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 116

- (Exam Topic 1)

What is the amount of fuel that should be on hand to power generators for backup datacenter power, in all tiers, according to the Uptime Institute?

- A. 1
- B. 1,000 gallons
- C. 12 hours
- D. As much as needed to ensure all systems may be gracefully shut down and data securely stored

**Answer:** C

#### NEW QUESTION 120

- (Exam Topic 1)

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 124

- (Exam Topic 1)

Impact resulting from risk being realized is often measured in terms of \_\_\_\_\_.

- A. Amount of data lost
- B. Money
- C. Amount of property lost
- D. Number of people affected

**Answer:** B

#### NEW QUESTION 129

- (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 134

- (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 136

- (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 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 139

- (Exam Topic 1)

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 140

- (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 142

- (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 145

- (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 149

- (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 152

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 156

- (Exam Topic 2)

Which SSAE 16 audit report is simply an attestation of audit results? Response:

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

**Answer:** D

#### NEW QUESTION 159

- (Exam Topic 2)

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

- A. User punishment
- B. Credential revocation
- C. Law enforcement notification
- D. Device tracking

**Answer:** B

#### NEW QUESTION 162

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 166

- (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 167

- (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 169

- (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 172

- (Exam Topic 2)

The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) addresses all the following security architecture elements except \_\_\_\_\_.  
Response:

- A. Physical security
- B. IaaS
- C. Application security
- D. Business drivers

**Answer:** D

#### NEW QUESTION 174

- (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 176

- (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 181

- (Exam Topic 2)

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 184

- (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 186**

- (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 190**

- (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 195**

- (Exam Topic 2)

Firewalls can detect attack traffic by using all these methods except \_\_\_\_\_.

Response:

- A. Known past behavior in the environment
- B. Identity of the malicious user
- C. Point of origination
- D. Signature matching

**Answer:** B

**NEW QUESTION 198**

- (Exam Topic 2)

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

Response:

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

**Answer:** D

**NEW QUESTION 199**

- (Exam Topic 2)

SOC 2 reports were intended to be \_\_\_\_\_.

Response:

- A. Released to the public
- B. Only technical assessments
- C. Retained for internal use
- D. Nonbinding

**Answer:** C

**NEW QUESTION 201**

- (Exam Topic 2)

You are the security manager for a company that is considering cloud migration to an IaaS environment. You are assisting your company's IT architects in constructing the environment. Which of the following options do you recommend?

Response:

- A. Unrestricted public access
- B. Use of a Type I hypervisor
- C. Use of a Type II hypervisor
- D. Enhanced productivity without encryption

**Answer:** B

#### NEW QUESTION 202

- (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 203

- (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 206

- (Exam Topic 2)

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

Response:

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

**Answer:** D

#### NEW QUESTION 207

- (Exam Topic 2)

What are the four cloud deployment models? Response:

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

**Answer:** D

#### NEW QUESTION 212

- (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 216

- (Exam Topic 2)

Which of the following contract terms most incentivizes the cloud provider to meet the requirements listed in the SLA?

Response:

- A. Regulatory oversight
- B. Financial penalties
- C. Performance details
- D. Desire to maintain customer satisfaction

**Answer:** B

#### NEW QUESTION 219

- (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 220

- (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 222

- (Exam Topic 2)

According to OWASP recommendations, active software security testing should include all of the following except \_\_\_\_\_. .

Response:

- A. Session initiation testing
- B. Input validation testing
- C. Testing for error handling
- D. Testing for weak cryptography

**Answer:** A

#### NEW QUESTION 227

- (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 231

- (Exam Topic 2)

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 235

- (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 240

- (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 241

- (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 246

- (Exam Topic 2)

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

Response:

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

**Answer: D**

#### NEW QUESTION 251

- (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 252

- (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 256

- (Exam Topic 2)

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

Response:

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

**Answer: D**

#### NEW QUESTION 259

- (Exam Topic 2)

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 260

- (Exam Topic 2)

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 264

- (Exam Topic 2)

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 266

- (Exam Topic 2)

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 270

- (Exam Topic 2)

\_\_\_\_\_ can often be the result of inadvertent activity. Response:

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

**Answer:** C

#### NEW QUESTION 274

- (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 277

- (Exam Topic 2)

Which of these characteristics of a virtualized network adds risks to the cloud environment? Response:

- A. Redundancy
- B. Scalability
- C. Pay-per-use
- D. Self-service

**Answer:** A

#### NEW QUESTION 282

- (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 286

- (Exam Topic 3)

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

Response:

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

**Answer:** A

#### NEW QUESTION 288

- (Exam Topic 3)

In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?

Response:

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

**Answer:** D

#### NEW QUESTION 291

- (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 296

- (Exam Topic 3)

During the assessment phase of a risk evaluation, what are the two types of tests that are performed? Response:

- A. Internal and external
- B. Technical and managerial
- C. Physical and logical
- D. Qualitative and quantitative

**Answer:** D

#### NEW QUESTION 299

- (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 302

- (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 304

- (Exam Topic 3)

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 306

- (Exam Topic 3)

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

Response:

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

**Answer:** B

#### NEW QUESTION 311

- (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 313

- (Exam Topic 3)

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

Response:

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

**Answer:** A

#### NEW QUESTION 317

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 321

- (Exam Topic 3)

A loosely coupled storage cluster will have performance and capacity limitations based on the \_\_\_\_\_.

Response:

- A. Physical backplane connecting it
- B. Total number of nodes in the cluster
- C. Amount of usage demanded
- D. The performance and capacity in each node

**Answer:** D

#### NEW QUESTION 325

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 326

- (Exam Topic 3)

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

Response:

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

**Answer: B**

#### NEW QUESTION 327

- (Exam Topic 3)

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

Response:

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

**Answer: C**

#### NEW QUESTION 329

- (Exam Topic 3)

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

What do we call this problem? Response:

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

**Answer: B**

#### NEW QUESTION 332

- (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 336

- (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 338

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 341

- (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 346

- (Exam Topic 3)

You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally.

Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes. Your company has decided to expand its business to include selling and monitoring life-support equipment for medical providers.

What characteristic do you need to ensure is offered by your cloud provider? Response:

- A. Full automation of security controls within the cloud data center
- B. Tier 4 of the Uptime Institute certifications
- C. Global remote access
- D. Prevention of ransomware infections

**Answer: B**

#### NEW QUESTION 350

- (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 352

- (Exam Topic 3)

What aspect of a Type 2 hypervisor involves additional security concerns that are not relevant with a Type 1 hypervisor?

Response:

- A. Reliance on a host operating system
- B. Auditing
- C. Proprietary software
- D. Programming languages

**Answer: A**

#### NEW QUESTION 354

- (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 357

- (Exam Topic 3)

Which type of web application monitoring most closely measures actual activity? Response:

- A. Synthetic performance monitoring
- B. Real-user monitoring (RUM)
- C. Security information and event management (SIEM)
- D. Database application monitor (DAM)

**Answer: B**

#### NEW QUESTION 360

- (Exam Topic 3)

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 365

- (Exam Topic 3)

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 370

- (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 372

- (Exam Topic 3)

A web application firewall (WAF) can understand and act on \_\_\_\_\_ traffic.

Response:

- A. Malicious
- B. SMTP
- C. ICMP
- D. HTTP

**Answer:** D

#### NEW QUESTION 373

- (Exam Topic 3)

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 377

- (Exam Topic 3) Who operates the management plane? Response:

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

**Answer:** C

#### NEW QUESTION 379

- (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 380

- (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 383

- (Exam Topic 3)

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 385

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 390

- (Exam Topic 3)

Security best practices in a virtualized network environment would include which of the following? Response:

- A. Using distinct ports and port groups for various VLANs on a virtual switch rather than running them through the same port
- B. Running iSCSI traffic unencrypted in order to have it observed and monitored by NIDS
- C. Adding HIDS to all virtual guests
- D. Hardening all outward-facing firewalls in order to make them resistant to attack

**Answer:** A

#### NEW QUESTION 391

- (Exam Topic 3)

You work for a government research facility. Your organization often shares data with other government research organizations.

You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations.

Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.

In order to pass the user IDs and authenticating credentials of each user among the organizations, what protocol/language/motif will you most likely utilize? Response:

- A. Representational State Transfer (REST)
- B. Security Assertion Markup Language (SAML)
- C. Simple Object Access Protocol (SOAP)
- D. Hypertext Markup Language (HTML)

**Answer:** B

#### NEW QUESTION 392

- (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 395

- (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 396

- (Exam Topic 3)

\_\_\_\_\_ is perhaps the main external factor driving IAM efforts. Response:

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

**Answer: A**

#### NEW QUESTION 400

- (Exam Topic 3)

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

Response:

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

**Answer: B**

#### NEW QUESTION 401

- (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 402

- (Exam Topic 3)

Setting thermostat controls by measuring the temperature will result in the \_\_\_\_\_ highest energy costs. Response:

- A. Server inlet
- B. Return air
- C. Under-floor
- D. External ambient

**Answer: B**

#### NEW QUESTION 404

.....

## 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