

CCSP Dumps

Certified Cloud Security Professional

<https://www.certleader.com/CCSP-dumps.html>



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)

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

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

Answer: C

NEW QUESTION 3

- (Exam Topic 1)

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

Response:

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

Answer: A

NEW QUESTION 4

- (Exam Topic 1) What can tokenization be used for? Response:

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

Answer: B

NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 9

- (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 10

- (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 10

- (Exam Topic 1)

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 14

- (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 15

- (Exam Topic 1)

Which of the following best describes data masking? Response:

- A. A method where the last few numbers in a dataset are not obscure
- B. These are often used for authentication.
- C. A method for creating similar but inauthentic datasets used for software testing and user training.
- D. A method used to protect prying eyes from data such as social security numbers and credit card data.
- E. Data masking involves stripping out all similar digits in a string of numbers so as to obscure the original number.

Answer: B

NEW QUESTION 19

- (Exam Topic 1)

A typical DLP tool can enhance the organization's efforts at accomplishing what legal task? Response:

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

Answer: A

NEW QUESTION 22

- (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 23

- (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 26

- (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 31

- (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 35

- (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 38

- (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 41

- (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 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 44

- (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 45

- (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 47

- (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 51

- (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 54

- (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 59

- (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 60

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 63

- (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 64

- (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 69

- (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 74

- (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 77

- (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 79

- (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 84

- (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 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 88

- (Exam Topic 1)

A firewall can use all of the following techniques for controlling traffic except:

- A. Rule sets
- B. Behavior analysis
- C. Content filtering
- D. Randomization

Answer: D

NEW QUESTION 90

- (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 94

- (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 95

- (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 99

- (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 101

- (Exam Topic 1) 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 106

- (Exam Topic 1)

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 108

- (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 109

- (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 110

- (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 115

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 117

- (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 119

- (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 120

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 121

- (Exam Topic 1)

A honeypot should contain data_____.

Response:

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

Answer: C

NEW QUESTION 123

- (Exam Topic 1)

Who will determine data classifications for the cloud customer?

- A. The cloud provider
- B. NIST
- C. Regulators
- D. The cloud customer

Answer: D

NEW QUESTION 128

- (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 131

- (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 136

- (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 139

- (Exam Topic 1)

_____ is the most prevalent protocol used in identity federation.

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

Answer: B

NEW QUESTION 144

- (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 146

- (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 151

- (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 152

- (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 154

- (Exam Topic 2)

Which of the following is the best example of a key component of regulated PII? Response:

- A. Items that should be implemented
- B. Mandatory breach reporting
- C. Audit rights of subcontractors
- D. PCI DSS

Answer: B

NEW QUESTION 158

- (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 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)

A bare-metal hypervisor is Type _____.

Response:

- A. 1
- B. 2

- C. 3
- D. 4

Answer: A

NEW QUESTION 170

- (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 174

- (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 177

- (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 180

- (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 181

- (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 185

- (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 188

- (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 191

- (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 196

- (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 198

- (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 200

- (Exam Topic 2)

What is the risk to the organization posed by dashboards that display data discovery results? Response:

- A. Increased chance of external penetration
- B. Flawed management decisions based on massaged displays
- C. Higher likelihood of inadvertent disclosure
- D. Raised incidence of physical theft

Answer: B

NEW QUESTION 201

- (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 202

- (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 205

- (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 210

- (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 215

- (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 216

- (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 221

- (Exam Topic 2)

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

Response:

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

Answer: D

NEW QUESTION 223

- (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 224

- (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 226

- (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 227

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 228

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 231

- (Exam Topic 2)

What aspect of data center planning occurs first? Response:

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

Answer: B

NEW QUESTION 235

- (Exam Topic 2)

Which of the following is a risk associated with manual patching especially in the cloud? Response:

- A. No notice before the impact is realized
- B. Lack of applicability to the environment
- C. Patches may or may not address the vulnerability they were designed to fix.
- D. The possibility for human error

Answer: D

NEW QUESTION 237

- (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 239

- (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 244

- (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 248

- (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 249

- (Exam Topic 2)

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 251

- (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 253

- (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 255

- (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 259

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 262

- (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 264

- (Exam Topic 2)

Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality? Response:

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

Answer: C

NEW QUESTION 268

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 272

- (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 273

- (Exam Topic 3)

You work for a company that operates a production environment in the cloud. Another company using the same cloud provider is under investigation by law

enforcement for racketeering.

Your company should be concerned about this because of the cloud characteristic of . Response:

- A. Virtualization
- B. Pooled resources
- C. Elasticity
- D. Automated self-service

Answer: B

NEW QUESTION 278

- (Exam Topic 3)

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

This is an example of what?

Response:

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

Answer: C

NEW QUESTION 281

- (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 284

- (Exam Topic 3)

Which technology is most associated with tunneling? Response:

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

Answer: B

NEW QUESTION 285

- (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 289

- (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 291

- (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 294

- (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 299

- (Exam Topic 3)

Which of the following threats from the OWASP Top Ten is the most difficult for an organization to protect against?

Response:

- A. Advanced persistent threats
- B. Account hijacking
- C. Malicious insiders
- D. Denial of service

Answer: C

NEW QUESTION 300

- (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 304

- (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 307

- (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 311

- (Exam Topic 3)

Cloud environments are based entirely on virtual machines and virtual devices, and those images are also in need of storage within the environment. What type of storage is typically used for virtual images?

Response:

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

Answer: D

NEW QUESTION 315

- (Exam Topic 3)

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

Response:

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

Answer: D

NEW QUESTION 318

- (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 321

- (Exam Topic 3)

A truly airgapped machine selector will _____.

Response:

- A. Terminate a connection before creating a new connection
- B. Be made of composites and not metal
- C. Have total Faraday properties
- D. Not be portable

Answer: A

NEW QUESTION 322

- (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 324

- (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 325

- (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 329

- (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 334

- (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 336

- (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 339

- (Exam Topic 3)

There are two reasons to conduct a test of the organization's recovery from backup in an environment other than the primary production environment. Which of the following is one of them? Response:

- A. It is good to invest in more than one community.
- B. You want to approximate contingency conditions, which includes not operating in the primary location.
- C. It is good for your personnel to see other places occasionally.
- D. Your regulators won't follow you offsite, so you'll be unobserved during your test.

Answer: B

NEW QUESTION 341

- (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 342

- (Exam Topic 3)

Tokenization requires two distinct _____.

Response:

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

Answer: B

NEW QUESTION 347

- (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 348

- (Exam Topic 3)

Which ISO/IEC standards set documents the cloud definitions for staffing and official roles? Response:

- A. ISO/IEC 27001
- B. ISO/IEC 17788
- C. ISO/IEC 17789
- D. ISO/IEC 27040

Answer: B

NEW QUESTION 350

- (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 352

- (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 353

- (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 354

- (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 359

- (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 360

- (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 365

- (Exam Topic 3)

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

Response:

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

Answer: B

NEW QUESTION 369

- (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 373

- (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 374

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 376

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 377

- (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 382

- (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 386

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CCSP Exam with Our Prep Materials Via below:

<https://www.certleader.com/CCSP-dumps.html>