

CCSP Dumps

Certified Cloud Security Professional

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



NEW QUESTION 1

- (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 2

- (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 3

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 4

- (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 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 best describes SAML? Response:

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

Answer: B

NEW QUESTION 7

- (Exam Topic 1)

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

Response:

- A. Contract
- B. Operational level agreement

- C. Service level agreement
- D. Regulation

Answer: C

NEW QUESTION 8

- (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 9

- (Exam Topic 1)

You are in charge of creating the BCDR plan and procedures for your organization. Your organization has its production environment hosted by a cloud provider, and you have appropriate protections in place.

Which of the following is a significant consideration for your BCDR backup? Response:

- A. Enough personnel at the BCDR recovery site to ensure proper operations
- B. Good cryptographic key management
- C. Access to the servers where the BCDR backup is stored
- D. Forensic analysis capabilities

Answer: B

NEW QUESTION 10

- (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 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 19

- (Exam Topic 1)

Egress monitoring solutions usually include a function that _____.

Response:

- A. Uses biometrics to scan users
- B. Inspects incoming packets
- C. Resides on client machines
- D. Uses stateful inspection

Answer: C

NEW QUESTION 21

- (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 25

- (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 30

- (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 35

- (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 36

- (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 41

- (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 44

- (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 49

- (Exam Topic 1)

Which of the following storage types are used with an Infrastructure as a Service (IaaS) solution? Response:

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

Answer: D

NEW QUESTION 54

- (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 57

- (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 61

- (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 62

- (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 63

- (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 68

- (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 72

- (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 77

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 82

- (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)

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)

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 92

- (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 93

- (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 96

- (Exam Topic 1)

All of the following are terms used to describe the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:
Response:

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

Answer: B

NEW QUESTION 101

- (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 105

- (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 110

- (Exam Topic 1)

Log data should be protected _____.

Response:

- A. One level below the sensitivity level of the systems from which it was collected
- B. At least at the same sensitivity level as the systems from which it was collected
- C. With encryption in transit, at rest, and in use
- D. According to NIST guidelines

Answer: B

NEW QUESTION 115

- (Exam Topic 1)

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

Response:

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

Answer: B

NEW QUESTION 120

- (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 121

- (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 124

- (Exam Topic 1)

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

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

Response:

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

Answer: D

NEW QUESTION 129

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 132

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 135

- (Exam Topic 1)

Who is the entity identified by personal data? Response:

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

Answer: D

NEW QUESTION 138

- (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 143

- (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 144

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 145

- (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 147

- (Exam Topic 1)

Which of the following best describes a cloud carrier?

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

Answer: B

NEW QUESTION 151

- (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 155

- (Exam Topic 1)

Heating, ventilation, and air conditioning (HVAC) systems cool the data center by pushing warm air into _____.

Response:

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

Answer: D

NEW QUESTION 160

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 161

- (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 165

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 167

- (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 171

- (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 173

- (Exam Topic 2)

What could be the result of failure of the cloud provider to secure the hypervisor in such a way that one user on a virtual machine can see the resource calls of another user's virtual machine?

Response:

- A. Unauthorized data disclosure
- B. Inference attacks
- C. Social engineering
- D. Physical intrusion

Answer: B

NEW QUESTION 177

- (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 180

- (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 182

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 184

- (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 186

- (Exam Topic 2)

A bare-metal hypervisor is Type _____.

Response:

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

Answer: A

NEW QUESTION 191

- (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 194

- (Exam Topic 2)

Your organization has made it a top priority that any cloud environment being considered to host production systems have guarantees that resources will always be available for allocation when needed.

Which of the following concepts will you need to ensure is part of the contract and SLA? Response:

- A. Limits
- B. Shares
- C. Resource pooling
- D. Reservations

Answer: D

NEW QUESTION 196

- (Exam Topic 2)

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

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

Response:

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

Answer: C

NEW QUESTION 197

- (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 202

- (Exam Topic 2)

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

Response:

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

Answer: B

NEW QUESTION 206

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 209

- (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 213

- (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 215

- (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 218

- (Exam Topic 2)

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

Response:

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

Answer: C

NEW QUESTION 219

- (Exam Topic 2)

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

Response:

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

Answer: D

NEW QUESTION 223

- (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 227

- (Exam Topic 2)

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

Response:

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

Answer: D

NEW QUESTION 230

- (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 231

- (Exam Topic 2)

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

Response:

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

Answer: C

NEW QUESTION 236

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 239

- (Exam Topic 2)

Why does the physical location of your data backup and/or BCDR failover environment matter? Response:

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

Answer: A

NEW QUESTION 241

- (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 245

- (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 249

- (Exam Topic 2)

Tokenization requires at least _____ database(s).

Response:

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

Answer: B

NEW QUESTION 253

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 255

- (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 257

- (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 258

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

Answer: B

NEW QUESTION 263

- (Exam Topic 2)

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

Response:

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

Answer: B

NEW QUESTION 268

- (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 269

- (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 270

- (Exam Topic 2)

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

- A. It poses a threat to health and human safety when deployed.

- B. It can harm the environment.
- C. It does not adequately suppress fires.
- D. It causes undue damage to electronic systems.

Answer: B

NEW QUESTION 273

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 277

- (Exam Topic 2)

Each of the following is an element of the Identification phase of the identity and access management (IAM) process except _____.

Response:

- A. Provisioning
- B. Inversion
- C. Management
- D. Deprovisioning

Answer: B

NEW QUESTION 282

- (Exam Topic 2)

What type of software is often considered secured and validated via community knowledge?

Response:

- A. Proprietary
- B. Object-oriented
- C. Open source
- D. Scripting

Answer: C

NEW QUESTION 286

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 288

- (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 290

- (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 292

- (Exam Topic 2)

Which of the following in a federated environment is responsible for consuming authentication tokens? Response:

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

Answer: A

NEW QUESTION 296

- (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 301

- (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 306

- (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 308

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 312

- (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 317

- (Exam Topic 2)

What is a cloud storage architecture that manages the data in caches of copied content close to locations of high demand? Response:

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

Answer: D

NEW QUESTION 318

- (Exam Topic 2)

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

Response:

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

Answer: B

NEW QUESTION 323

- (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 328

- (Exam Topic 2)

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

Response:

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

Answer: D

NEW QUESTION 332

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 333

- (Exam Topic 2)

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

Response:

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

Answer: B

NEW QUESTION 338

- (Exam Topic 2)

You are the IT director for a small contracting firm. Your company is considering migrating to a cloud production environment.

Which service model would best fit your needs if you wanted an option that reduced the chance of vendor lock-in but also did not require the highest degree of administration by your own personnel?

Response:

- A. IaaS
- B. PaaS

- C. SaaS
- D. TanstaafL

Answer: B

NEW QUESTION 343

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 345

- (Exam Topic 2)

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

Response:

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

Answer: A

NEW QUESTION 347

- (Exam Topic 3)

Why might an organization choose to comply with the ISO 27001 standard? Response:

Response:

- A. Price
- B. Ease of implementation
- C. International acceptance
- D. Speed

Answer: C

NEW QUESTION 351

- (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 353

- (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:

Response:

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

Answer: C

NEW QUESTION 356

- (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 358

- (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 359

- (Exam Topic 3)

Access should be based on _____.

Response:

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

Answer: B

NEW QUESTION 363

- (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 366

- (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 368

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 371

- (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 372

- (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 377

- (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 379

- (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 382

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 386

- (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 389

- (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 390

- (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 394

- (Exam Topic 3)

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

Response:

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

Answer: C

NEW QUESTION 399

- (Exam Topic 3)

DLP solutions can aid in deterring loss due to which of the following?

Response:

- A. Randomization
- B. Inadvertent disclosure
- C. Natural disaster
- D. Device failure

Answer: B

NEW QUESTION 404

- (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 405

- (Exam Topic 3)

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

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

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

Answer: D

NEW QUESTION 407

- (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 410

- (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 415

- (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 417

- (Exam Topic 3)

Dynamic application security testing (DAST) is usually considered a _____ form of testing. Response:
White-box

- A. Parched field
- B. Black-box
- C. Gray-box
- D. Parched field

Answer: B

NEW QUESTION 419

- (Exam Topic 3)

Anonymization is the process of removing from data sets. Response:

- A. Access
- B. Cryptographic keys
- C. Numeric values
- D. Identifying information

Answer: D

NEW QUESTION 422

- (Exam Topic 3)

Tokenization requires two distinct _____.
Response:

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

Answer: B

NEW QUESTION 425

- (Exam Topic 3)

Which characteristic of automated patching makes it attractive? Response:

- A. Cost
- B. Speed
- C. Noise reduction
- D. Capability to recognize problems quickly

Answer: B

NEW QUESTION 427

- (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 429

- (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 431

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 434

- (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 439

- (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 443

- (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 444

- (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 447

- (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 450

- (Exam Topic 3)

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

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

Response:

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

Answer: B

NEW QUESTION 452

- (Exam Topic 3)

Alice is the CEO for a software company; she is considering migrating the operation from the current on-premises legacy environment into the cloud.

In order to protect her company's intellectual property, Alice might want to consider implementing all these techniques/solutions except _____.

Response:

- A. Egress monitoring
- B. Encryption
- C. Turnstiles
- D. Digital watermarking

Answer: C

NEW QUESTION 455

- (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 460

- (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 465

- (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 466

- (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 468

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 471

- (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 472

- (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 476

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 478

- (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 482

.....

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>