ISC2

Exam Questions CCSP

Certified Cloud Security Professional

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
_____ can often be the result of inadvertent activity. Response:

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

Answer: C

NEW QUESTION 4
- (Exam Topic 1)
Which strategy involves using a fake production system to lure attackers in order to learn about their tactics?
Response:

A. IDS
B. Honeypot
C. IPS
D. Firewall

Answer: B

NEW QUESTION 5
- (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 6
- (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 7
- (Exam Topic 1)
Which of the following is characterized by a set maximum capacity? Response:

A. A secret-sharing-made-short (SSMS) bit-splitting implementation

B. A tightly coupled cloud storage cluster
C. A loosely coupled cloud storage cluster
D. A public-key infrastructure

Answer: B

NEW QUESTION 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)
Which of the following should occur at each stage of the SDLC?

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

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
What is the federal agency that accepts applications for new patents?

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

Answer: B

NEW QUESTION 10
- (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 15
- (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 16
- (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 18

- (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 20
- (Exam Topic 1)
Which phase of the cloud data lifecycle involves processing by a user or application? Response:

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

Answer: D

NEW QUESTION 24
- (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 29
- (Exam Topic 1)
Which of the following are contractual components that the CSP should review and understand fully when contracting with a cloud service provider? (Choose two.)

A. Concurrently maintainable site infrastructure
B. Use of subcontractors
C. Redundant site infrastructure capacity components
D. Scope of processing

Answer: BD

NEW QUESTION 34
- (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 39
- (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 42
- (Exam Topic 1)
Which of the following tools might be useful in data discovery efforts that are based on content analysis?

A. DLP

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

Answer: A

NEW QUESTION 47
- (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 52
- (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 56
- (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 61
- (Exam Topic 1)
Which of the following types of organizations is most likely to make use of open source software technologies?

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

Answer: C

NEW QUESTION 62
- (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 63
- (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 64

- (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 66
- (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 71
- (Exam Topic 1)
You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Management is interested in adopting an Agile development style.
This will be typified by which of the following traits? Response:

A. Reliance on a concrete plan formulated during the Define phase
B. Rigorous, repeated security testing
C. Isolated programming experts for specific functional elements
D. Short, iterative work periods

Answer: D

NEW QUESTION 72
- (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 76
- (Exam Topic 1)
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:
Response:

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

Answer: B

NEW QUESTION 81
- (Exam Topic 1)
Which of the following top security threats involves attempting to send invalid commands to an application in an attempt to get the application to execute the code?
Response:

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

Answer: B

NEW QUESTION 86
- (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 88
- (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 91
- (Exam Topic 1)
The physical layout of a cloud data center campus should include redundancies of all the following except _____ .
Response:

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

Answer: D

NEW QUESTION 96
- (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 98
- (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 101
- (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 104
- (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 106
- (Exam Topic 1)
Which ISO standard refers to addressing security risks in a supply chain?

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

Answer: B

NEW QUESTION 107
- (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 108
- (Exam Topic 1)
Which of the following is not an enforceable governmental request? Response:

A. Warrant
B. Subpoena
C. Court order
D. Affidavit

Answer: D

NEW QUESTION 110
- (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 114
- (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 115
- (Exam Topic 1)
Impact resulting from risk being realized is often measured in terms of _____.

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

Answer: B

NEW QUESTION 116
- (Exam Topic 1)
Application virtualization can typically be used for .

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

Answer:

D

NEW QUESTION 117
- (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 119
- (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 122
- (Exam Topic 1)
The Cloud Security Alliance (CSA) publishes, the Notorious Nine, a list of common threats to organizations participating in cloud computing.
According to the CSA, all of the following activity can result in data loss except _____ .

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

Answer: B

NEW QUESTION 127
- (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 132
- (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 133
- (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 135
- (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 139
- (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 144
- (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 146
- (Exam Topic 2)
A process for _____ can aid in protecting against data disclosure due to lost devices. Response:

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

Answer: B

NEW QUESTION 148
- (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 152
- (Exam Topic 2)
In a Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a _____.
Response:

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

Answer: B

NEW QUESTION 154
- (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 158
- (Exam Topic 2)
Which type of cloud service category would having a vendor-neutral encryption scheme for data at rest (DAR) be the MOST important?
Response:

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

Answer: B

NEW QUESTION 163
- (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 168
- (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 173
- (Exam Topic 2)
Which of the following are not examples of personnel controls? Response:

A. Background checks
B. Reference checks
C. Strict access control mechanisms
D. Continuous security training

Answer: C

NEW QUESTION 177
- (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 179
- (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 181
- (Exam Topic 2)
The physical layout of a cloud data center campus should include redundancies of all the following except _____ .
Response:

A. Physical perimeter security controls (fences, lights, walls, etc.)
B. The administration/support staff building
C. Electrical utility lines
D. Communications connectivity lines

Answer: B

NEW QUESTION 184
- (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 186
- (Exam Topic 2)
Which of the following is a method for apportioning resources that involves setting maximum usage amounts for all tenants/customers within the environment? Response:

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

Answer: D

NEW QUESTION 191
- (Exam Topic 2)
All of the following entitles are required to use FedRAMP-accredited Cloud Service Providers except _____.
Response:

A. The US post office
B. The Department of Homeland Security
C. Federal Express
D. The CIA

Answer: C

NEW QUESTION 195
- (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 198
- (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 202
- (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 206
- (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 211
- (Exam Topic 2) What does nonrepudiation mean?
Response:

A. Prohibiting certain parties from a private conversation
B. Ensuring that a transaction is completed before saving the results
C. Ensuring that someone cannot turn off auditing capabilities while performing a function
D. Preventing any party that participates in a transaction from claiming that it did not

Answer: D

NEW QUESTION 212
- (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 inproduction systems
C. Include the baseline image in the asset inventory/configuration management database
D. Configure the host OS according to the baseline requirements

Answer: C

NEW QUESTION 216
- (Exam Topic 2)
Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider? Response:

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

Answer: D

NEW QUESTION 220
- (Exam Topic 2)
In application-level encryption, where does the encryption engine reside? Response:

A. In the application accessing the database
B. In the OS on which the application is run
C. Within the database accessed by the application
D. In the volume where the database resides

Answer: A

NEW QUESTION 225
- (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 matte
E. Data can be saved anywhere without consequence

Answer: A

NEW QUESTION 226

- (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 227
- (Exam Topic 2)
Tokenization requires at least _____ database(s).
Response:

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

Answer: B

NEW QUESTION 230
- (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 233
- (Exam Topic 2)
Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?
Response:

A. Systems
B. Data
C. Cash
D. Personnel

Answer: C

NEW QUESTION 238
- (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 241
- (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 246
- (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 248
- (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 249
- (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 253
- (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 256
- (Exam Topic 2)
What is a form of cloud storage where data is stored as objects, arranged in a hierarchal structure, like a file tree?
Response:

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

Answer: D

NEW QUESTION 261
- (Exam Topic 2)
All of the following are identity federation standards commonly found in use today except _____.
Response:

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

Answer: D

NEW QUESTION 263
- (Exam Topic 2)
What are the phases of a software development lifecycle process model? Response:

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

Answer: A

NEW QUESTION 264
- (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 265
- (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 269
- (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 270
- (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 274
- (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 277
- (Exam Topic 2)
All of the following methods can be used to attenuate the harm caused by escalation of privilege except: Response:

A. Extensive access control and authentication tools and techniques
B. Analysis and review of all log data by trained, skilled personnel on a frequent basis
C. Periodic and effective use of cryptographic sanitization tools
D. The use of automated analysis tools such as SIM, SIEM, and SEM solutions

Answer: C

NEW QUESTION 278
- (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 283
- (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 285
- (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 287
- (Exam Topic 2)
_____ can often be the result of inadvertent activity. Response:

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

Answer: C

NEW QUESTION 291
- (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 296
- (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 298
- (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 299
- (Exam Topic 2)
The tasks performed by the hypervisor in the virtual environment can most be likened to the tasks of the _____ in the legacy environment.
Response:

A. Central processing unit (CPU)
B. Security team
C. OS
D. PGP

Answer: A

NEW QUESTION 300
- (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 302
- (Exam Topic 3)
Why might an organization choose to comply with the ISO 27001 standard?
Response:

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

Answer: C

NEW QUESTION 304
- (Exam Topic 3)
Federation allows _____ across organizations.
Response:

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

Answer: D

NEW QUESTION 306
- (Exam Topic 3)
Cloud vendors are held to contractual obligations with specified metrics by:
Response:

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

Answer: A

NEW QUESTION 311
- (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 314
- (Exam Topic 3)
Which of the following methods for the safe disposal of electronic records can always be used in a cloud environment? Response:

A. Physical destruction
B. Encryption
C. Overwriting
D. Degaussing

Answer: B

NEW QUESTION 316
- (Exam Topic 3)
Devices in the cloud datacenter should be secure against attack. All the following are means of hardening devices, except:
Response:

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

Answer: D

NEW QUESTION 318
- (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 323
- (Exam Topic 3)
Digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM) often protect unauthorized distribution of what type of intellectual property?
Response:

A. Patents
B. Trademarks
C. Personally identifiable information (PII)
D. Copyright

Answer: D

NEW QUESTION 324
- (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 325
- (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 330
- (Exam Topic 3)
A cloud provider is looking to provide a higher level of assurance to current and potential cloud customers about the design and effectiveness of their security controls.
Which of the following audit reports would the cloud provider choose as the most appropriate to accomplish this goal?
Response:

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

Answer: D

NEW QUESTION 332

- (Exam Topic 3)
Digital rights management (DRM) tools can be combined with _____, to enhance security capabilities. Response:

A. Roaming identity services (RIS)
B. Egress monitoring solutions (DLP)
C. Internal hardware settings (BIOS)
D. Remote Authentication Dial-In User Service (RADIUS)

Answer: B

NEW QUESTION 337
- (Exam Topic 3)
When a customer performs a penetration test in the cloud, why isn't the test an optimum simu-lation 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 338
- (Exam Topic 3)
Which of the following is not a component of the of the STRIDE model? Response:

A. Spoofing
B. Repudiation
C. Information disclosure
D. External pen testing

Answer: D

NEW QUESTION 340
- (Exam Topic 3)
Which type of cloud-based storage is IRM typically associated with? Response:

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

Answer: D

NEW QUESTION 341
- (Exam Topic 3)
Which of the following data-sanitation approaches are always available within a cloud environment? Response:

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

Answer: D

NEW QUESTION 345
- (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 348
- (Exam Topic 3)
Proper _____ need to be assigned to each data classification/category. Response:

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

Answer: C

NEW QUESTION 353
- (Exam Topic 3)
Which of the following is an example of useful and sufficient data masking of the string “CCSP”? Response:

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

Answer: C

NEW QUESTION 354
- (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 359
- (Exam Topic 3)
Which of the following would NOT be used to determine the classification of data?
Response:

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

Answer: D

NEW QUESTION 362
- (Exam Topic 3)
DLP solutions can aid all of the following security-related efforts except _____.
Response:

A. Access control
B. Egress monitoring
C. e-discovery/forensics
D. Data categorization/classification

Answer: A

NEW QUESTION 367
- (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 369
- (Exam Topic 3)
When using an Infrastructure as a Service (IaaS) solution, what is the capability provided to the customer? Response:

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

Answer: D

NEW QUESTION 372
- (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 376
- (Exam Topic 3)
You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally.
Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes. Your company has decided to expand its business to include selling and monitoring life-support equipment for medical providers.
What characteristic do you need to ensure is offered by your cloud provider? Response:

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

Answer: B

NEW QUESTION 378
- (Exam Topic 3)
What is the major difference between authentication/authorization? Response:

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

Answer: B

NEW QUESTION 380
- (Exam Topic 3)
What aspect of a Type 2 hypervisor involves additional security concerns that are not relevant with a Type 1 hypervisor?
Response:

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

Answer: A

NEW QUESTION 381
- (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 385
- (Exam Topic 3)
What type of identity system allows trust and verifications between the authentication systems of multiple organizations?
Response:

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

Answer: A

NEW QUESTION 390
- (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 394
- (Exam Topic 3)
Which type of web application monitoring most closely measures actual activity? Response:

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

Answer: B

NEW QUESTION 399
- (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 403
- (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 406
- (Exam Topic 3)
Tokenization requires two distinct _____.
Response:

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

Answer: B

NEW QUESTION 408
- (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 411
- (Exam Topic 3)
What are the objectives of change management? (Choose all that apply.)
Response:

A. Respond to a customer's changing business requirements while maximizing value and reducing incidents, disruption, and rework
B. Ensure that changes are recorded and evaluated
C. Respond to business and IT requests for change that will disassociate services with business needs
D. Ensure that all changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner

Answer: AB

NEW QUESTION 416
- (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 418
- (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 421
- (Exam Topic 3)
In which of the following situations does the data owner have to administer the OS? Response:

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

Answer: A

NEW QUESTION 426
- (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 431
- (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 433
- (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 435
- (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 437
- (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 440
- (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 441
- (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 445
.....

Relate Links

100% Pass Your CCSP Exam with Exambible Prep Materials

https://www.exambible.com/CCSP-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/