ISC2

Exam Questions CCSP

Certified Cloud Security Professional

NEW QUESTION 1
- (Exam Topic 1)
Vulnerability scans are dependent on _____ in order to function. Response:

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

Answer: B

NEW QUESTION 2
- (Exam Topic 1)
A virtual network interface card (NIC) exists at layer _____ of the OSI model. Response:

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

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
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 4
- (Exam Topic 1) What can tokenization be used for? Response:

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

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
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)
Which of the following is essential for getting full security value from your system baseline? Response:

A. Capturing and storing an image of the baseline
B. Keeping a copy of upcoming suggested modifications to the baseline
C. Having the baseline vetted by an objective third party
D. Using a baseline from another industry member so as not to engage in repetitious efforts

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
When an organization implements an SIEM solution and begins aggregating event data, the configured event sources are only valid at the time it was configured. Application modifications, patching, and other upgrades will change the events generated and how they are represented over time.
What process is necessary to ensure events are collected and processed with this in mind?

A. Continual review
B. Continuous optimization

C. Aggregation updates
D. Event elasticity

Answer: B

NEW QUESTION 8
- (Exam Topic 1)
Which concept of cloud computing pertains to the ability to reuse components and services of an application for other purposes?

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

Answer: B

NEW QUESTION 9
- (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 10
- (Exam Topic 1)
Of the following, which is probably the most significant risk in a managed cloud environment? Response:

A. DDoS
B. Management plane breach
C. Guest escape
D. Physical attack on the utility service lines

Answer: B

NEW QUESTION 13
- (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 15
- (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 20
- (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 23
- (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)
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “cross-site scripting (XSS).” Which of the following is not a method for reducing the risk of XSS attacks? Response:

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

Answer: B

NEW QUESTION 30
- (Exam Topic 1)
Who is ultimately responsible for a data breach that includes personally identifiable information (PII), in the event of negligence on the part of the cloud provider?

A. The user
B. The subject
C. The cloud provider
D. The cloud customer

Answer: D

NEW QUESTION 35
- (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 39
- (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 40
- (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 43
- (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 45
- (Exam Topic 1)
TLS uses _____ to authenticate a connection and create a shared secret for the duration of the session.

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

Answer: B

NEW QUESTION 49
- (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 52
- (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 54
- (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 57
- (Exam Topic 1)
You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider.
Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also allow users to select which APIs they install and use on their own devices in order to access and manipulate company data.
Of the following, what is a security control you'd like to implement to offset the risk(s) incurred by this practice?

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

Answer: A

NEW QUESTION 60
- (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 65
- (Exam Topic 1)
Which type of report is considered for “general” use and does not contain any sensitive information? Response:

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

Answer: C

NEW QUESTION 66
- (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 69
- (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 74
- (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 75
- (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 77
- (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 79
- (Exam Topic 1)
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing?
Response:

A. Most of the cloud customer's interaction with resources will be performed through APIs.
B. APIs are inherently insecure.
C. Attackers have already published vulnerabilities for all known APIs.
D. APIs are known carcinogens.

Answer: A

NEW QUESTION 80
- (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 82
- (Exam Topic 1)
During which stage of the SDLC process should security be consulted and begin its initial involvement?

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

Answer: D

NEW QUESTION 86
- (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 90
- (Exam Topic 1)
DRM solutions should generally include all the following functions, except:

A. Persistency
B. Automatic self-destruct
C. Automatic expiration
D. Dynamic policy control

Answer: B

NEW QUESTION 94
- (Exam Topic 1)
You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Previous releases have shipped with major flaws that were not detected in the testing phase; leadership wants to avoid repeating that problem. What tool/technique/technology might you suggest to aid in identifying programming errors?

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

Answer: B

NEW QUESTION 99

- (Exam Topic 1)
A honeypot should contain data_____.
Response:

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

Answer: C

NEW QUESTION 100
- (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 104
- (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 106
- (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 109
- (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 114
- (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 119
- (Exam Topic 1)
What are the six components that make up the STRIDE threat model? Response:

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

D. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Social Engineering

Answer: A

NEW QUESTION 120
- (Exam Topic 2)
Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?
Response:

A. Mapping to existing access control lists (ACLs)
B. Delineating biometric catalogs
C. Preventing multifactor authentication
D. Prohibiting unauthorized transposition

Answer: A

NEW QUESTION 122
- (Exam Topic 2)
What is the intellectual property protection for the logo of a new video game? Response:

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

Answer: C

NEW QUESTION 123
- (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 125
- (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 129
- (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 134
- (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 137
- (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 141
- (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 142
- (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 144
- (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 148
- (Exam Topic 2)
Which one of the following is not one of the three common threat modeling techniques? Response:

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

Answer: D

NEW QUESTION 153
- (Exam Topic 2)
Although encryption can help an organization to effectively decrease the possibility of data breaches, which other type of threat can it increase the chances of?
Response:

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

Answer: B

NEW QUESTION 158
- (Exam Topic 2)
Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?
Response:

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

Answer: A

NEW QUESTION 162
- (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 167
- (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 168
- (Exam Topic 2)
Although performing BCDR tests at regular intervals is a best practice to ensure processes and documentation are still relevant and efficient, which of the following represents a reason to conduct a BCDR review outside of the regular interval?
Response:

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

Answer: B

NEW QUESTION 169
- (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 174
- (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 175
- (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 177
- (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 181
- (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 186
- (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 187
- (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 191
- (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 196
- (Exam Topic 2)
Tokenization requires at least _____ database(s).
Response:

A. One
B. Two

C. Three
D. Four

Answer: B

NEW QUESTION 201
- (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 204
- (Exam Topic 2)
Single sign-on systems work by authenticating users from a centralized location or using a centralized method, and then allowing applications that trust the system to grant those users access. What would be passed between the authentication system and the applications to grant a user access?
Response:

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

Answer: D

NEW QUESTION 207
- (Exam Topic 2)
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 208
- (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 209
- (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 214
- (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 215

- (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 220
- (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 221
- (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 223
- (Exam Topic 2)
Which security certification serves as a general framework that can be applied to any type of system or application?
Response:

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

Answer: A

NEW QUESTION 228
- (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 233
- (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 234
- (Exam Topic 2)
You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider’s data center.
One of the challenges you’re facing is whether the provider will have undue control over your data once it is within the provider’s data center; will the provider be able to hold your organization hostage because they have your data?
This is a(n) _____ issue. Response:

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

Answer: B

NEW QUESTION 238
- (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 241
- (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 244
- (Exam Topic 2)
Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company's website)?
Response:

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

Answer: D

NEW QUESTION 245
- (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 247
- (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 250
- (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 252
- (Exam Topic 2)
You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization.
What is probably the best benefit offered by the CCM? Response:

A. The low cost of the tool
B. Allowing your organization to leverage existing controls across multiple frameworks so as not to duplicate effort
C. Simplicity of control selection from the list of approved choices
D. Ease of implementation by choosing controls from the list of qualified vendors

Answer: B

NEW QUESTION 257
- (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 258
- (Exam Topic 2)
Which of the following is a method for apportioning resources that involves prioritizing resource requests to resolve contention situations?
Response:

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

Answer: B

NEW QUESTION 259
- (Exam Topic 2)
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 262
- (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 264
- (Exam Topic 2)
Which of the following data protection methodologies maintains the ability to connect back values to the original values?
Response:

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

Answer: A

NEW QUESTION 265

- (Exam Topic 2)
Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality? Response:

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

Answer: C

NEW QUESTION 270
- (Exam Topic 2)
Which of the following is not a way to manage risk? Response:

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

Answer: A

NEW QUESTION 272
- (Exam Topic 2)
Designers making applications for the cloud have to take into consideration risks and operational constraints that did not exist or were not as pronounced in the legacy environment.
Which of the following is an element cloud app designers may have to consider incorporating in software for the cloud that might not have been as important in the legacy environment?
Response:

A. IAM capability
B. DDoS resistance
C. Encryption for data at rest and in motion
D. Field validation

Answer: C

NEW QUESTION 275
- (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 279
- (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 280
- (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 282
- (Exam Topic 3)
A user signs on to a cloud-based social media platform. In another browser tab, the user finds an article worth posting to the social media platform. The user clicks on the platform's icon listed on the article's website, and the article is automatically posted to the user's account on the social media platform.
This is an example of what?
Response:

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

Answer: C

NEW QUESTION 287
- (Exam Topic 3)
Which network protocol is essential for allowing automation and orchestration within a cloud environment? Response:

A. DNSSEC
B. DHCP
C. IPsec
D. VLANs

Answer: B

NEW QUESTION 290
- (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 295
- (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 296
- (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 299
- (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 304
- (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 305

- (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 309
- (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 314
- (Exam Topic 3)
A truly airgapped machine selector will _____.
Response:

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

Answer: A

NEW QUESTION 319
- (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 324
- (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 325
- (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 329
- (Exam Topic 3)
When a user accesses a system, what process determines the roles and privileges that user is granted within the application?

Response:

A. Authorization
B. Authentication
C. Provisioning
D. Privilege

Answer: A

NEW QUESTION 330
- (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 333
- (Exam Topic 3)
It's important to maintain a current asset inventory list, including surveying your environment on a regular basis, in order to _____ .
Response:

A. Prevent unknown, unpatched assets from being used as back doors to the environment
B. Ensure that any lost devices are automatically entered into the acquisition system for repurchasing and replacement
C. Maintain user morale by having their devices properly catalogued and annotated
D. Ensure that billing for all devices is handled by the appropriate departments

Answer: A

NEW QUESTION 335
- (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 337
- (Exam Topic 3)
Tokenization requires two distinct _____.
Response:

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

Answer: B

NEW QUESTION 339
- (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 343
- (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 345
- (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 346
- (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 348
- (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 351
- (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 352
- (Exam Topic 3)
In addition to BCDR, what other benefit can your data archive/backup provide? Response:

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

Answer: D

NEW QUESTION 357
- (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 359
- (Exam Topic 3)

You work for a government research facility. Your organization often shares data with other government research organizations.
You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations.
Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.
In order to pass the user IDs and authenticating credentials of each user among the organizations, what protocol/language/motif will you most likely utilize? Response:

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

Answer: B

NEW QUESTION 360
- (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 365
- (Exam Topic 3)
Managed cloud services exist because the service is less expensive for each customer than creating the same services for themselves in a legacy environment. Using a managed service allows the customer to realize significant cost savings through the reduction of _____.
Response:

A. Risk
B. Security controls
C. Personnel
D. Data

Answer: C

NEW QUESTION 370
- (Exam Topic 3)
Your application has been a continued target for SQL injection attempts. Which of the following technologies would be best used to combat the likeliness of a successful SQL injection exploit from occurring?
Response:

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

Answer: B

NEW QUESTION 371
- (Exam Topic 3)
The BIA can be used to provide information about all the following, except: Response:

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

Answer: B

NEW QUESTION 376
- (Exam Topic 3)
Software-defined networking (SDN) is intended to separate different network capabilities and allow for the granting of granular configurations, permissions, and features to non-network staff or customers. Which network capability is separated from forwarding of traffic?
Response:

A. Routing
B. Firewalling
C. Filtering
D. IPS

Answer: C

NEW QUESTION 379
- (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 380
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CCSP Practice Exam Features:

* CCSP Questions and Answers Updated Frequently

* CCSP Practice Questions Verified by Expert Senior Certified Staff

* CCSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CCSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year