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 4)
Which of the following is considered a physical control?

A. Fences
B. Ceilings
C. Carpets
D. Doors

Answer: A

Explanation:
Fences are physical controls; carpets and ceilings are architectural features, and a door is not necessarily a control: the lock on the door would be a physical security control. Although you might think of a door as a potential answer, the best answer is the fence; the exam will have questions where more than one answer is correct, and the answer that will score you points is the one that is most correct.

NEW QUESTION 2
- (Exam Topic 4)
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the required amount of time to restore services to the predetermined level?

A. RPO
B. RSL
C. RTO
D. SRE

Answer: C

Explanation:
The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the predetermined level of operations necessary during a BCDR situation. SRE is provided as an erroneous response.

NEW QUESTION 3
- (Exam Topic 4)
Which of the following are distinguishing characteristics of a managed service provider?

A. Be able to remotely monitor and manage objects for the customer and proactively maintain these objects under management.
B. Have some form of a help desk but no NOC.
C. Be able to remotely monitor and manage objects for the customer and reactively maintain these objects under management.
D. Have some form of a NOC but no help desk.

Answer: A

Explanation:
According to the MSP Alliance, typically MSPs have the following distinguishing characteristics:
- Have some form of NOC service
- Have some form of help desk service
- Can remotely monitor and manage all or a majority of the objects for the customer
- Can proactively maintain the objects under management for the customer
- Can deliver these solutions with some form of predictable billing model, where the customer knows with great accuracy what her regular IT management expense will be

NEW QUESTION 4
- (Exam Topic 4)
Which of the following is the best example of a key component of regulated PII?

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

Answer: D

Explanation:
Mandatory breach reporting is the best example of regulated PII components. The rest are generally considered components of contractual PII.

NEW QUESTION 5
- (Exam Topic 4)
Which cloud service category most commonly uses client-side key management systems?

A. Software as a Service
B. Infrastructure as a Service
C. Platform as a Service
D. Desktop as a Service

Answer: A

Explanation:
SaaS most commonly uses client-side key management. With this type of implementation, the software for doing key management is supplied by the cloud provider, but is hosted and run by the cloud customer. This allows for full integration with the SaaS implementation, but also provides full control to the cloud customer. Although the cloud provider may offer software for performing key management to the cloud customers, with the Infrastructure, Platform, and Desktop as a Service categories, the customers would largely be responsible for their own options and implementations and would not be bound by the offerings from the cloud provider.

NEW QUESTION 6
- (Exam Topic 4)
Which ITIL component focuses on ensuring that system resources, processes, and personnel are properly allocated to meet SLA requirements?

A. Continuity management
B. Availability management
C. Configuration management
D. Problem management

Answer: B

Explanation:
Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Configuration management tracks and maintains detailed information about all IT components within an organization. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION 7
- (Exam Topic 4)
What are the U.S. State Department controls on technology exports known as?

A. DRM
B. ITAR
C. EAR
D. EAL

Answer: B

Explanation:
ITAR is a Department of State program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Digital rights management tools are used for protecting electronic processing of intellectual property.

NEW QUESTION 8
- (Exam Topic 4)
Tokenization requires two distinct _____.

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

Answer: D

Explanation:
In order to implement tokenization, there will need to be two databases: the database containing the raw, original data, and the token database containing tokens that map to original data. Having two-factor authentication is nice, but certainly not required. Encryption keys are not necessary for tokenization. Two-person integrity does not have anything to do with tokenization.

NEW QUESTION 9
- (Exam Topic 4)
In addition to battery backup, a UPS can offer which capability?

A. Breach alert
B. Confidentiality
C. Communication redundancy
D. Line conditioning

Answer: D

Explanation:
A UPS can provide line conditioning, adjusting power so that it is optimized for the devices it serves and smoothing any power fluctuations; it does not offer any of the other listed functions.

NEW QUESTION 10
- (Exam Topic 4)
Which of the following best describes the Organizational Normative Framework (ONF)?

A. A set of application security, and best practices, catalogued and leveraged by the organization

B. A container for components of an application's security, best practices catalogued and leveraged by the organization
C. A framework of containers for some of the components of application security, best practices, catalogued and leveraged by the organization
D. A framework of containers for all components of application security, best practices, catalogued and leveraged by the organization.

Answer: D

Explanation:
Option B is incorrect, because it refers to a specific applications security elements, meaning it is about an ANF, not the ONF. C is true, but not as complete as D, making D the better choice. C suggests that the framework contains only "some" of the components, which is why B (which describes "all" components) is better

NEW QUESTION 10
- (Exam Topic 4)
Cloud systems are increasingly used for BCDR solutions for organizations. What aspect of cloud computing makes their use for BCDR the most attractive?

A. On-demand self-service
B. Measured service
C. Portability
D. Broad network access

Answer: B

Explanation:
Business continuity and disaster recovery (BCDR) solutions largely sit idle until they are actually needed. This traditionally has led to increased costs for an organization because physical hardware must be purchased and operational but is not used. By using a cloud system, an organization will only pay for systems when they are being used and only for the duration of use, thus eliminating the need for extra hardware and costs. Portability is the ability to easily move services among different cloud providers. Broad network access allows access to users and staff from anywhere and from different clients, and although this would be important for a BCDR situation, it is not the best answer in this case. On-demand self-service allows users to provision services automatically and when needed, and although this too would be important for BCDR situations, it is not the best answer because it does not address costs or the biggest benefits to an organization.

NEW QUESTION 14
- (Exam Topic 4)
Which data sanitation method is also commonly referred to as "zeroing"?

A. Overwriting
B. Nullification
C. Blanking
D. Deleting

Answer: A

Explanation:
The zeroing of data--or the writing of null values or arbitrary data to ensure deletion has been fully completed--is officially referred to as overwriting. Nullification, deleting, and blanking are provided as distractor terms.

NEW QUESTION 16
- (Exam Topic 4)
What is the intellectual property protection for the tangible expression of a creative idea?

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

Answer: B

Explanation:
Copyrights are protected tangible expressions of creative works. The other answers listed are answers to subsequent questions.

NEW QUESTION 17
- (Exam Topic 4)
What is an experimental technology that is intended to create the possibility of processing encrypted data without having to decrypt it first?

A. Quantum-state
B. Polyinstantiation
C. Homomorphic
D. Gastronomic

Answer: C

Explanation:
Homomorphic encryption hopes to achieve that goal; the other options are terms that have almost nothing to do with encryption.

NEW QUESTION 19
- (Exam Topic 4)
What concept does the D represent within the STRIDE threat model?

A. Denial of service
B. Distributed
C. Data breach
D. Data loss

Answer: A

Explanation:
Any application can be a possible target of denial of service (DoS) attacks. From the application side, the developers should minimize how many operations are performed for unauthenticated users. This will keep the application running as quickly as possible and using the least amount of system resources to help minimize the impact of any such attacks. None of the other options provided is the correct term.

NEW QUESTION 20
- (Exam Topic 4)
Which component of ITIL involves handling anything that can impact services for either internal or public users?

A. Incident management
B. Deployment management
C. Problem management
D. Change management

Answer: A

Explanation:
Incident management is focused on limiting the impact of disruptions to an organization's services or operations, as well as returning their state to full operational status as soon as possible. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur. Deployment management is a subcomponent of change management and is where the actual code or configuration change is put into place. Change management involves the processes and procedures that allow an organization to make changes to its IT systems and services in a controlled manner.

NEW QUESTION 23
- (Exam Topic 4)
What is the intellectual property protection for a useful manufacturing innovation?

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

Answer: C

Explanation:
Patents protect processes (as well as inventions, new plantlife, and decorative patterns). The other answers listed are answers to other questions.

NEW QUESTION 25
- (Exam Topic 4)
As a result of scandals involving publicly traded corporations such as Enron, WorldCom, and Adelphi, Congress passed legislation known as:

A. SOX
B. HIPAA
C. FERPA
D. GLBA

Answer: A

Explanation:
Sarbanes-Oxley was a direct response to corporate scandals. FERPA is related to education. GLBA is about the financial industry. HIPAA is about health care.

NEW QUESTION 29
- (Exam Topic 4)
All the following are data analytics modes, except:

A. Datamining
B. Agile business intelligence
C. Refractory iterations
D. Real-time analytics

Answer: C

Explanation:
All the others are data analytics methods, but “refractory iterations” is a nonsense term thrown in as a red herring.

NEW QUESTION 31
- (Exam Topic 4)
An audit scope statement defines the limits and outcomes from an audit.
Which of the following would NOT be included as part of an audit scope statement?

A. Reports
B. Certification
C. Billing
D. Exclusions

Answer: C

Explanation:
Billing for an audit, or other cost-related items, would not be part of an audit scope statement and would instead be handled prior to the actual audit as part of the contract between the organization and auditors. Reports, exclusions to the scope of the audit, and required certifications on behalf of the systems or auditors are all crucial elements of an audit scope statement.

NEW QUESTION 32
- (Exam Topic 4)
Which of the following is NOT a major regulatory framework?

A. PCI DSS
B. HIPAA
C. SOX
D. FIPS 140-2

Answer: D

Explanation:
FIPS 140-2 is a United States certification standard for cryptographic modules, and it provides guidance and requirements for their use based on the requirements of the data classification. However, these are not actual regulatory requirements. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS) are all major regulatory frameworks either by law or specific to an industry.

NEW QUESTION 36
- (Exam Topic 4)
What is the correct order of the phases of the data life cycle?

A. Create, Use, Store, Share, Archive, Destroy
B. Create, Archive, Store, Share, Use, Destroy
C. Create, Store, Use, Archive, Share, Destroy
D. Create, Store, Use, Share, Archive, Destroy

Answer: D

Explanation:
The other options are the names of the phases, but out of proper order.

NEW QUESTION 39
- (Exam Topic 4)
All policies within the organization should include a section that includes all of the following, except:

A. Policy adjudication
B. Policy maintenance
C. Policy review
D. Policy enforcement

Answer: A

Explanation:
All the elements except adjudication need to be addressed in each policy. Adjudication is not an element of policy.

NEW QUESTION 43
- (Exam Topic 4)
Cryptographic keys should be secured _____.

A. To a level at least as high as the data they can decrypt
B. In vaults
C. With two-person integrity
D. By armed guards

Answer: A

Explanation:
The physical security of crypto keys is of some concern, but guards or vaults are not always necessary.
Two-person integrity might be a good practice for protecting keys. The best answer to this question is option A, because it is always true, whereas the remaining options depend on circumstances.

NEW QUESTION 44
- (Exam Topic 4)
Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider?

A. SOC 1 Type 1

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

Answer: C

Explanation:
The SOC 3 is the least detailed, so the provider is not concerned about revealing it. The SOC 1 Types 1 and 2 are about financial reporting, and not relevant. The SOC 2 Type 2 is much more detailed and will most likely be kept closely held by the provider.

NEW QUESTION 48
- (Exam Topic 4)
When an organization is considering a cloud environment for hosting BCDR solutions, which of the following would be the greatest concern?

A. Self-service
B. Resource pooling
C. Availability
D. Location

Answer: D

Explanation:
If an organization wants to use a cloud service for BCDR, the location of the cloud hosting becomes a very important security consideration due to regulations and jurisdiction, which could be dramatically different from the organization's normal hosting locations. Availability is a hallmark of any cloud service provider, and likely will not be a prime consideration when an organization is considering using a cloud for BCDR; the same goes for self-service options. Resource pooling is common among all cloud systems and would not be a concern when an organization is dealing with the provisioning of resources during a disaster.

NEW QUESTION 50
- (Exam Topic 4)
Because cloud providers will not give detailed information out about their infrastructures and practices to the general public, they will often use established auditing reports to ensure public trust, where the reputation of the auditors serves for assurance.
Which type of audit reports can be used for general public trust assurances?

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

Answer: C

Explanation:
SOC Type 3 audit reports are very similar to SOC Type 2, with the exception that they are intended for general release and public audiences.SAS-70 audits have been deprecated. SOC Type 1 audit reports have a narrow scope and are intended for very limited release, whereas SOC Type 2 audit reports are intended for wider audiences but not general release.

NEW QUESTION 55
- (Exam Topic 4)
Which format is the most commonly used standard for exchanging information within a federated identity system?

A. XML
B. HTML
C. SAML
D. JSON

Answer: C

Explanation:
Security Assertion Markup Language (SAML) is the most common data format for information exchange within a federated identity system. It is used to transmit and exchange authentication and authorization data.XML is similar to SAML, but it's used for general-purpose data encoding and labeling and is not used for the exchange of authentication and authorization data in the way that SAML is for federated systems. JSON is used similarly to XML, as a text-based data exchange format that typically uses attribute-value pairings, but it's not used for authentication and authorization exchange. HTML is used only for encoding web pages for web browsers and is not used for data exchange--and certainly not in a federated system.

NEW QUESTION 57
- (Exam Topic 4)
For performance purposes, OS monitoring should include all of the following except:

A. Disk space
B. Disk I/O usage
C. CPU usage
D. Print spooling

Answer: D

Explanation:
Print spooling is not a metric for system performance; all the rest are.

NEW QUESTION 61
- (Exam Topic 4)
The goals of DLP solution implementation include all of the following, except:

A. Elasticity
B. Policy enforcement
C. Data discovery
D. Loss of mitigation

Answer: A

Explanation:
DLP does not have anything to do with elasticity, which is the capability of the environment to scale up or down according to demand. All the rest are goals of DLP implementations.

NEW QUESTION 64
- (Exam Topic 4)
When using a PaaS solution, what is the capability provided to the customer?

A. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the provider support
B. The provider does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
C. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the provider support
D. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
E. To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools that the consumer support
F. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
G. To deploy onto the cloud infrastructure provider-created or acquired applications created using programming languages, libraries, services, and tools that the provider support
H. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Answer: B

Explanation:
According to “The NIST Definition of Cloud Computing,” in PaaS, “the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the
application-hosting environment.

NEW QUESTION 65
- (Exam Topic 4)
Which of the following methods of addressing risk is most associated with insurance?

A. Mitigation
B. Transference
C. Avoidance
D. Acceptance

Answer: B

Explanation:
Avoidance halts the business process, mitigation entails using controls to reduce risk, acceptance involves taking on the risk, and transference usually involves insurance.

NEW QUESTION 70
- (Exam Topic 4)
What concept does the A represent within the DREAD model?

A. Affected users
B. Authorization
C. Authentication
D. Affinity

Answer: A

Explanation:
The concept of affected users measures the percentage of users who would be impacted by a successful exploit. Scoring ranges from 0, which would impact no users, to 10, which would impact all users. None of the other options provided is the correct term.

NEW QUESTION 73
- (Exam Topic 4)
What is the experimental technology that might lead to the possibility of processing encrypted data without having to decrypt it first?

A. AES
B. Link encryption
C. One-time pads
D. Homomorphic encryption

Answer: D

Explanation:
AES is an encryption standard. Link encryption is a method for protecting communications traffic. One-time pads are an encryption method.

NEW QUESTION 74
- (Exam Topic 4)
Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:

A. The cloud provider's utilities
B. The cloud provider's suppliers
C. The cloud provider's resellers
D. The cloud provider's vendors

Answer: C

Explanation:
The cloud provider's resellers are a marketing and sales mechanism, not an operational dependency that could affect the security of a cloud customer.

NEW QUESTION 78
- (Exam Topic 4)
Which of the following is NOT one of the components of multifactor authentication?

A. Something the user knows
B. Something the user has
C. Something the user sends
D. Something the user is

Answer: C

Explanation:
Multifactor authentication systems are composed of something the user knows, has, and/or is, not something the user sends. Multifactor authentication commonly uses something that a user knows, has, and/or is (such as biometrics or features).

NEW QUESTION 80
- (Exam Topic 4)
Data masking can be used to provide all of the following functionality, except:

A. Secure remote access
B. test data in sandboxed environments
C. Authentication of privileged users
D. Enforcing least privilege

Answer: C

Explanation:
Data masking does not support authentication in any way. All the others are excellent use cases for data masking.

NEW QUESTION 84
- (Exam Topic 4)
When reviewing the BIA after a cloud migration, the organization should take into account new factors related to data breach impacts. One of these new factors is:

A. Many states have data breach notification laws.
B. Breaches can cause the loss of proprietary data.
C. Breaches can cause the loss of intellectual property.
D. Legal liability can't be transferred to the cloud provider.

Answer: D

Explanation:
State notification laws and the loss of proprietary data/intellectual property pre-existed the cloud; only the lack of ability to transfer liability is new.

NEW QUESTION 88
- (Exam Topic 4)
Gathering business requirements can aid the organization in determining all of this information about organizational assets, except:

A. Full inventory
B. Criticality
C. Value
D. Usefulness

Answer: D

Explanation:
When we gather information about business requirements, we need to do a complete inventory, receive accurate valuation of assets (usually from the owners of those assets), and assess criticality; this collection of information does not tell us, objectively, how useful an asset is, however.

NEW QUESTION 90
- (Exam Topic 4)
Which of the following terms is not associated with cloud forensics?

A. eDiscovery
B. Chain of custody
C. Analysis
D. Plausibility

Answer: D

Explanation:
Plausibility, here, is a distractor and not specifically relevant to cloud forensics.

NEW QUESTION 94
- (Exam Topic 4)
Best practices for key management include all of the following, except:

A. Ensure multifactor authentication
B. Pass keys out of band
C. Have key recovery processes
D. Maintain key security

Answer: A

Explanation:
We should do all of these except for requiring multifactor authentication, which is pointless in key management.

NEW QUESTION 96
- (Exam Topic 4)
Which type of testing uses the same strategies and toolsets that hackers would use?

A. Static
B. Malicious
C. Penetration
D. Dynamic

Answer: C

Explanation:
Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discovery potential vulnerabilities. Although the term malicious captures much of the intent of penetration testing from the perspective of an attacker, it is not the best answer. Static and dynamic are two types of system testing--where static is done offline and with knowledge of the system, and dynamic is done on a live system without any previous knowledge is associated--but neither describes the type of testing being asked for in the question.

NEW QUESTION 101
- (Exam Topic 4)
The goals of SIEM solution implementation include all of the following, except:

A. Dashboarding
B. Performance enhancement
C. Trend analysis
D. Centralization of log streams

Answer: B

Explanation:
SIEM does not intend to provide any enhancement of performance; in fact, a SIEM solution may decrease performance because of additional overhead. All the rest are goals of SIEM implementations.

NEW QUESTION 103
- (Exam Topic 4)
Which ITIL component is focused on anticipating predictable problems and ensuring that configurations and operations are in place to prevent these problems from ever occurring?

A. Availability management
B. Continuity management
C. Configuration management
D. Problem management

Answer: D

Explanation:

Problem management is focused on identifying and mitigating known problems and deficiencies before they are able to occur, as well as on minimizing the impact of incidents that cannot be prevented. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Configuration management tracks and maintains detailed information about all IT components within an organization.

NEW QUESTION 108
- (Exam Topic 4)
To protect data on user devices in a BYOD environment, the organization should consider requiring all the following, except:

A. Multifactor authentication
B. DLP agents
C. Two-person integrity
D. Local encryption

Answer: C

Explanation:
Although all the other options are ways to harden a mobile device, two-person integrity is a concept that has nothing to do with the topic, and, if implemented, would require everyone in your organization to walk around in pairs while using their mobile devices.

NEW QUESTION 113
- (Exam Topic 4)
Many aspects of cloud computing bring enormous benefits over a traditional data center, but also introduce new challenges unique to cloud computing.
Which of the following aspects of cloud computing makes appropriate data classification of high importance?

A. Multitenancy
B. Interoperability
C. Portability
D. Reversibility

Answer: A

Explanation:
With multitenancy, where different cloud customers all share the same physical systems and networks, data classification becomes even more important to ensure that the appropriate security controls are applied immediately to prevent any potential leakage or exposure to other customers. Portability refers to the ability to move easily from one cloud provider to another. Interoperability refers to the ability to reuse components and services for different uses. Reversibility refers to the ability of the cloud customer to quickly and completely remove all data and services from a cloud provider and to verify the removal.

NEW QUESTION 114
- (Exam Topic 4)
Which of the following components are part of what a CCSP should review when looking at contracting with a cloud service provider?

A. Redundant uplink grafts
B. Background checks for the provider’s personnel
C. The physical layout of the datacenter
D. Use of subcontractors

Answer: D

Explanation:
The use of subcontractors can add risk to the supply chain and should be considered; trusting the provider’s management of their vendors and suppliers (including subcontractors) is important to trusting the provider. Conversely, the customer is not likely to be allowed to review the physical design of the datacenter (or, indeed, even know the exact location of the datacenter) or the personnel security specifics for the provider’s staff. “Redundant uplink grafts” is a nonsense term used as a distractor.

NEW QUESTION 116
- (Exam Topic 4)
Which of the following is the dominant driver behind the regulations to which a system or application must adhere?

A. Data source
B. Locality
C. Contract
D. SLA

Answer: B

Explanation:
The locality--or physical location and jurisdiction where the system or data resides--is the dominant driver of regulations. This may be based on the type of data contained within the application or the way in which the data is used. The contract and SLA both articulate requirements for regulatory compliance and the responsibilities for the cloud provider and cloud customer, but neither artifact defines the actual requirements. Instead, the contract and SLA merely form the official documentation between the cloud provider and cloud customer. The source of the data may place contractual requirements or best practice guidelines on its usage, but ultimately jurisdiction has legal force and greater authority.

NEW QUESTION 121
- (Exam Topic 4)
Just like the risk management process, the BCDR planning process has a defined sequence of steps and processes to follow to ensure the production of a comprehensive and successful plan.

Which of the following is the correct sequence of steps for a BCDR plan?

A. Define scope, gather requirements, assess risk, implement
B. Define scope, gather requirements, implement, assess risk
C. Gather requirements, define scope, implement, assess risk
D. Gather requirements, define scope, assess risk, implement

Answer: A

Explanation:
The correct sequence for a BCDR plan is to define the scope, gather requirements based on the scope, assess overall risk, and implement the plan. The other sequences provided are not in the correct order.

NEW QUESTION 122
- (Exam Topic 4)
What category of PII data can carry potential fines or even criminal charges for its improper use or disclosure?

A. Protected
B. Legal
C. Regulated
D. Contractual

Answer: C

Explanation:
Regulated PII data carries legal and jurisdictional requirements, along with official penalties for its misuse or disclosure, which can be either civil or criminal in nature. Legal and protected are similar terms, but neither is the correct answer in this case. Contractual requirements can carry financial or contractual impacts for the improper use or disclosure of PII data, but not legal or criminal penalties that are officially enforced.

NEW QUESTION 123
- (Exam Topic 4)
Which protocol, as a part of TLS, handles the actual secure communications and transmission of data?

A. Negotiation
B. Handshake
C. Transfer
D. Record

Answer: D

Explanation:
The TLS record protocol is the actual secure communications method for transmitting data; it's responsible for encrypting and authenticating packets throughout their transmission between the parties, and in some cases it also performs compression. The TLS handshake protocol is what negotiates and establishes the TLS connection between two parties and enables the secure communications channel to then handle data transmissions. Negotiation and transfer are not protocols under TLS.

NEW QUESTION 125
- (Exam Topic 4)
When an organization is considering the use of cloud services for BCDR planning and solutions, which of the following cloud concepts would be the most important?

A. Reversibility
B. Elasticity
C. Interoperability
D. Portability

Answer: D

Explanation:
Portability is the ability for a service or system to easily move among different cloud providers. This is essential for using a cloud solution for BCDR because vendor lock-in would inhibit easily moving and setting up services in the event of a disaster, or it would necessitate a large number of configuration or component changes to implement. Interoperability, or the ability to reuse components for other services or systems, would not be an important factor for BCDR. Reversibility, or the ability to remove all data quickly and completely from a cloud environment, would be important at the end of a disaster, but would not be important during setup and deployment. Elasticity, or the ability to resize resources to meet current demand, would be very beneficial to a BCDR situation, but not as vital as portability.

NEW QUESTION 128
- (Exam Topic 4)
BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the amount of data and services needed to reach the predetermined level of operations?

A. SRE
B. RPO
C. RSL
D. RTO

Answer: B

Explanation:

The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the predetermined level of operations necessary during a BCDR situation. The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. SRE is provided as an erroneous response.

NEW QUESTION 132
- (Exam Topic 4)
Which of the following best describes the purpose and scope of ISO/IEC 27034-1?

A. Describes international privacy standards for cloud computing
B. Serves as a newer replacement for NIST 800-52 r4
C. Provides on overview of network and infrastructure security designed to secure cloud applications.
D. Provides an overview of application security that introduces definitive concepts, principles, and processes involved in application security.

Answer: D

NEW QUESTION 136
- (Exam Topic 4)
Which of the following is not an example of a highly regulated environment?

A. Financial services
B. Healthcare
C. Public companies
D. Wholesale or distribution

Answer: D

Explanation:
Wholesalers or distributors are generally not regulated, although the products they sell may be.

NEW QUESTION 138
- (Exam Topic 4)
Which of the following is considered a technological control?

A. Firewall software
B. Firing personnel
C. Fireproof safe
D. Fire extinguisher

Answer: A

Explanation:
A firewall is a technological control. The safe and extinguisher are physical controls and firing someone is an administrative control.

NEW QUESTION 143
- (Exam Topic 4)
There are many situations when testing a BCDR plan is appropriate or mandated. Which of the following would not be a necessary time to test a BCDR plan?

A. After software updates
B. After regulatory changes
C. After major configuration changes
D. Annually

Answer: B

Explanation:
Regulatory changes by themselves would not trigger a need for new testing of a BCDR plan. Any changes necessary for regulatory compliance would be accomplished through configuration changes or software updates, which in turn would then trigger the necessary new testing. Annual testing is crucial to any BCDR plan. Also, any time major configuration changes or software updates are done, the plan should be evaluated and tested to ensure it is still valid and complete.

NEW QUESTION 147
- (Exam Topic 4)
Which component of ITIL pertains to planning, coordinating, executing, and validating changes and rollouts to production environments?

A. Release management
B. Availability management
C. Problem management
D. Change management

Answer: A

Explanation:
Release management involves planning, coordinating, executing, and validating changes and rollouts to the production environment. Change management is a higher-level component than release management and also involves stakeholder and management approval, rather than specifically focusing the actual release itself. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION 148
- (Exam Topic 4)
BCDR strategies do not typically involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the amount of services that need to be recovered to meet BCDR objectives?

A. RSL
B. RTO
C. RPO
D. SRE

Answer: A

Explanation:
The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the determined level of operations necessary during a BCDR situation. The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. SRE is provided as an erroneous response.

NEW QUESTION 149
- (Exam Topic 4)
In the cloud motif, the data processor is usually:

A. The cloud customer
B. The cloud provider
C. The cloud access security broker
D. The party that assigns access rights

Answer: B

Explanation:
In legal terms, when “data processor” is defined, it refers to anyone who stores, handles, moves, or manipulates data on behalf of the data owner or controller. In the cloud computing realm, this is the cloud provider.

NEW QUESTION 151
- (Exam Topic 4)
What is the cloud service model in which the customer is responsible for administration of the OS?

A. QaaS
B. SaaS
C. PaaS
D. IaaS

Answer: D

Explanation:
In IaaS, the cloud provider only owns the hardware and supplies the utilities. The customer is responsible for the OS, programs, and data. In PaaS and SaaS, the provider also owns the OS. There is no QaaS. That is a red herring.

NEW QUESTION 156
- (Exam Topic 4)
What must SOAP rely on for security since it does not provide security as a built-in capability?

A. Encryption
B. Tokenization
C. TLS
D. SSL

Answer: A

Explanation:
Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for data passing, and it must rely on the encryption of those data packages for security. TLS and SSL (before it was deprecated) represent two commons approaches to using encryption for protection of data transmissions. However, they are only two possible options and do not encapsulate the overall concept the question is looking for. Tokenization, which involves the replacement of sensitive data with opaque values, would not be appropriate for use with SOAP because the actual data is needed by the services.

NEW QUESTION 157
- (Exam Topic 4)
Which of the following is the least challenging with regard to eDiscovery in the cloud?

A. Identifying roles such as data owner, controller and processor
B. Decentralization of data storage
C. Forensic analysis
D. Complexities of International law

Answer: C

Explanation:

Forensic analysis is the least challenging of the answers provided as it refers to the analysis of data once it is obtained. The challenges revolve around obtaining the data for analysis due to the complexities of international law, the decentralization of data storage or difficulty knowing where to look, and identifying the data owner, controller, and processor.

NEW QUESTION 161
- (Exam Topic 4)
What is the concept of isolating an application from the underlying operating system for testing purposes?

A. Abstracting
B. Application virtualization
C. Hosting
D. Sandboxing

Answer: B

Explanation:
Application virtualization is a software implementation that allows applications and programs to run in an isolated environment rather than directly interacting with the operating system. Sandboxing refers to segregating information or processes for security or testing purposes, but it's not directly related to isolation from the underlying operating system. Abstracting sounds similar to the correct term but is not pertinent to the question, and hosting is provided as an erroneous answer.

NEW QUESTION 162
- (Exam Topic 4)
Which of the following is considered an administrative control?

A. Keystroke logging
B. Access control process
C. Door locks
D. Biometric authentication

Answer: B

Explanation:
A process is an administrative control; sometimes, the process includes elements of other types of controls (in this case, the access control mechanism might be a technical control, or it might be a physical control), but the process itself is administrative. Keystroke logging is a technical control (or an attack, if done for malicious purposes, and not for auditing); door locks are a physical control; and biometric authentication is a technological control.

NEW QUESTION 165
- (Exam Topic 4)
Which of the following is the concept of segregating information or processes, within the same system or application, for security reasons?

A. Cell blocking
B. Sandboxing
C. Pooling
D. Fencing

Answer: B

Explanation:
Sandboxing involves the segregation and isolation of information or processes from other information or processes within the same system or application, typically for security concerns. Sandboxing is generally used for data isolation (for example, keeping different communities and populations of users isolated from others with similar data). In IT terminology, pooling typically means bringing together and consolidating resources or services, not segregating or separating them. Cell blocking and fencing are both erroneous terms.

NEW QUESTION 169
- (Exam Topic 4)
Every security program and process should have which of the following?

A. Severe penalties
B. Multifactor authentication
C. Foundational policy
D. Homomorphic encryption

Answer: C

Explanation:
Policy drives all programs and functions in the organization; the organization should not conduct any operations that don’t have a policy governing them. Penalties may or may not be an element of policy, and severity depends on the topic. Multifactor authentication and homomorphic encryption are red herrings here.

NEW QUESTION 171
- (Exam Topic 4)
Which of the following terms is NOT a commonly used category of risk acceptance?

A. Moderate
B. Critical
C. Minimal
D. Accepted

Answer:

D

Explanation:

Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

NEW QUESTION 172
- (Exam Topic 4)
Whereas a contract articulates overall priorities and requirements for a business relationship, which artifact enumerates specific compliance requirements, metrics, and response times?

A. Service level agreement
B. Service level contract
C. Service compliance contract
D. Service level amendment

Answer: A

Explanation:
The service level agreement (SLA) articulates minimum requirements for uptime, availability, processes, customer service and support, security controls, auditing requirements, and any other key aspect or requirement of the contract. Although the other choices sound similar to the correct answer, none is the proper term for this concept.

NEW QUESTION 176
- (Exam Topic 4)
Your company is in the planning stages of moving applications that have large data sets to a cloud environment.
What strategy for data removal would be the MOST appropriate for you to recommend if costs and speed are primary considerations?

A. Shredding
B. Media destruction
C. Crypthographic erasure
D. Overwriting

Answer: C

Explanation:
Cryptographic erasure involves having the data encrypted, typically as a matter of standard operations, and then rendering the data useless and unreadable by destroying the encryption keys for it. It represents a very cheap and immediate way to destroy data, and it works in all environments. With a cloud environment and multitenancy, media destruction or the physical destruction of storage devices, including shredding, would not be possible. Depending on the environment, overwriting may or may not be possible, but cryptographic erasure is the best answer because it is always an available option and is very quick to implement.

NEW QUESTION 179
- (Exam Topic 4)
Which of the following best describes a sandbox?

A. An isolated space where untested code and experimentation can safely occur separate from the production environment.
B. A space where you can safely execute malicious code to see what it does.
C. An isolated space where transactions are protected from malicious software
D. An isolated space where untested code and experimentation can safely occur within the production environment.

Answer: A

Explanation:
Options C and B are also correct, but A is more general and incorporates them both. D is incorrect, because sandboxing does not take place in the production environment.

NEW QUESTION 184
- (Exam Topic 4)
When beginning an audit, both the system owner and the auditors must agree on various aspects of the final audit report.
Which of the following would NOT be something that is predefined as part of the audit agreement?

A. Size
B. Format
C. Structure
D. Audience

Answer: A

Explanation:
The ultimate size of the audit report is not something that would ever be included in the audit scope or definition. Decisions about the content of the report should be the only factor that drives the ultimate size of the report. The structure, audience, and format of the audit report are all crucial elements that must be defined and agreed upon as part of the audit scope.

NEW QUESTION 185
- (Exam Topic 4)
Tokenization requires two distinct _____.

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

Answer: C

Explanation:
In order to implement tokenization, there will need to be two databases: the database containing the raw, original data, and the token database containing tokens that map to original data. Having two-factor authentication is nice, but certainly not required. Encryption keys are not necessary for tokenization. Two-person integrity does not have anything to do with tokenization.

NEW QUESTION 187
- (Exam Topic 3)
Where is a DLP solution generally installed when utilized for monitoring data in transit?

A. Network perimeter
B. Database server
C. Application server
D. Web server

Answer: A

Explanation:
To monitor data in transit, a DLP solution would optimally be installed at the network perimeter, to ensure that data leaving the network through various protocols conforms to security controls and policies. An application server or a web server would be more appropriate for monitoring data in use, and a database server would be an example of a location appropriate for monitoring data at rest.

NEW QUESTION 191
- (Exam Topic 3)
Modern web service systems are designed for high availability and resiliency. Which concept pertains to the ability to detect problems within a system, environment, or application and programmatically invoke redundant systems or processes for mitigation?

A. Elasticity
B. Redundancy
C. Fault tolerance
D. Automation

Answer: C

Explanation:
Fault tolerance allows a system to continue functioning, even with degraded performance, if portions of it fail or degrade, without the entire system or service being taken down. It can detect problems within a service and invoke compensating systems or functions to keep functionality going. Although redundancy is similar to fault tolerance, it is more focused on having additional copies of systems available, either active or passive, that can take up services if one system goes down. Elasticity pertains to the ability of a system to resize to meet demands, but it is not focused on system failures. Automation, and its role in maintaining large systems with minimal intervention, is not directly related to fault tolerance.

NEW QUESTION 192
- (Exam Topic 3)
Which of the following is considered an internal redundancy for a data center?

A. Power feeds
B. Chillers
C. Network circuits
D. Generators

Answer: B

Explanation:
Chillers and cooling systems are internal to a data center and its operations, and as such they are considered an internal redundancy. Power feeds, network circuits, and generators are all external to a data center and provide utility services to them, which makes them an external redundancy.

NEW QUESTION 195
- (Exam Topic 3)
With finite resources available within a cloud, even the largest cloud providers will at times need to determine which customers will receive additional resources first.
What is the term associated with this determination?

A. Weighting
B. Prioritization
C. Shares
D. Scoring

Answer: C

Explanation:
Shares are used within a cloud environment to prioritize resource allocation when customer requests exceed the available resources. Cloud providers utilize shares by assigning a priority score to each customer and allocating resources to those with the highest scores first. Scoring is a component of shares that

determines the actual order in which to allocate resources. Neither weighting nor prioritization is the correct term in this case.

NEW QUESTION 198
- (Exam Topic 3)
A DLP solution/implementation has three main components. Which of the following is NOT one of the three main components?

A. Monitoring
B. Enforcement
C. Auditing
D. Discovery and classification

Answer: C

Explanation:
Auditing, which can be supported to varying degrees by DLP solutions, is not a core component of them. Data loss prevention (DLP) solutions have core components of discovery and classification, enforcement, and monitoring. Discovery and classification are concerned with determining which data should be applied to the DLP policies, and then determining its classification level. Monitoring is concerned with the actual watching of data and how it's used through its various stages. Enforcement is the actual application of policies determined from the discovery stage and then triggered during the monitoring stage.

NEW QUESTION 201
- (Exam Topic 3)
Jurisdictions have a broad range of privacy requirements pertaining to the handling of personal data and information.
Which jurisdiction requires all storage and processing of data that pertains to its citizens to be done on hardware that is physically located within its borders?

A. Japan
B. United States
C. European Union
D. Russia

Answer: D

Explanation:
The Russian government requires all data and processing of information about its citizens to be done solely on systems and applications that reside within the physical borders of the country. The United States, European Union, and Japan focus their data privacy laws on requirements and methods for the protection of data, rather than where the data physically resides.

NEW QUESTION 206
- (Exam Topic 3)
If a key feature of cloud computing that your organization desires is the ability to scale and expand without limit or concern about available resources, which cloud deployment model would you MOST likely be considering?

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

Answer: A

Explanation:
Public clouds, such as AWS and Azure, are massive systems run by major corporations, and they account for a significant share of Internet traffic and services. They are always expanding, offer enormous resources to customers, and are the least likely to run into resource constraints compared to the other deployment models. Private clouds would likely have the resources available for specific uses and could not be assumed to have a large pool of resources available for expansion. A community cloud would have the same issues as a private cloud, being targeted to similar organizations. A hybrid cloud, because it spans multiple clouds, would not fit the bill either, without the use of individual cloud models.

NEW QUESTION 210
- (Exam Topic 3)
Within a federated identity system, which of the following would you be MOST likely to use for sending information for consumption by a relying party?

A. XML
B. HTML
C. WS-Federation
D. SAML

Answer: D

Explanation:
The Security Assertion Markup Language (SAML) is the most widely used method for encoding and sending attributes and other information from an identity provider to a relying party.WS-Federation, which is used by Active Directory Federation Services (ADFS), is the second most used method for sending information to a relying party, but it is not a better choice than SAML. XML is similar to SAML in the way it encodes and labels data, but it does not have all of the required extensions that SAML does. HTML is not used within federated systems at all.

NEW QUESTION 212
- (Exam Topic 3)
Which data state would be most likely to use digital signatures as a security protection mechanism?

A. Data in use
B. Data in transit

C. Archived
D. Data at rest

Answer: A

Explanation:
During the data-in-use state, the information has already been accessed from storage and transmitted to the service, so reliance on a technology such as digital signatures is imperative to ensure security and complement the security methods used during previous states. Data in transit relies on technologies such as TLS to encrypt network transmission of packets for security. Data at rest primarily uses encryption for stored file objects. Archived data would be the same as data at rest.

NEW QUESTION 213
- (Exam Topic 3)
Your boss has tasked your team with getting your legacy systems and applications connected with new cloud-based services that management has decided are crucial to customer service and offerings.
Which role would you be assuming under this directive?

A. Cloud service administrator
B. Cloud service user
C. Cloud service integrator
D. Cloud service business manager

Answer: C

Explanation:
The cloud service integrator role is responsible for connecting and integrating existing services and applications with cloud-based services.A cloud service administrator is responsible for testing, monitoring, and securing cloud services, as well as providing usage reporting and dealing with service problems. The cloud service user is someone who consumes cloud services. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

NEW QUESTION 215
- (Exam Topic 3)
Audits are either done based on the status of a system or application at a specific time or done as a study over a period of time that takes into account changes and processes.
Which of the following pairs matches an audit type that is done over time, along with the minimum span of time necessary for it?

A. SOC Type 2, one year
B. SOC Type 1, one year
C. SOC Type 2, one month
D. SOC Type 2, six months

Answer: D

Explanation:
SOC Type 2 audits are done over a period of time, with six months being the minimum duration. SOC Type 1 audits are designed with a scope that's a static point in time, and the other times provided for SOC Type 2 are incorrect.

NEW QUESTION 217
- (Exam Topic 3)
Which of the following threat types involves an application that does not validate authorization for portions of itself beyond when the user first enters it?

A. Cross-site request forgery
B. Missing function-level access control
C. Injection
D. Cross-site scripting

Answer: B

Explanation:
It is imperative that applications do checks when each function or portion of the application is accessed to ensure that the user is properly authorized. Without continual checks each time a function is accessed, an attacker could forge requests to access portions of the application where authorization has not been granted. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.

NEW QUESTION 219
- (Exam Topic 3)
If a company needed to guarantee through contract and SLAs that a cloud provider would always have available sufficient resources to start their services and provide a certain level of provisioning, what would the contract need to refer to?

A. Limit
B. Reservation
C. Assurance
D. Guarantee

Answer: B

Explanation:

A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources. A limit refers to the enforcement of a maximum level of resources that can be consumed by or allocated to a cloud customer, service, or system. Both guarantee and assurance are terms that sound similar to reservation, but they are not correct choices.

NEW QUESTION 220
- (Exam Topic 3)
Within an IaaS implementation, which of the following would NOT be a metric used to quantify service charges for the cloud customer?

A. Memory
B. Number of users
C. Storage
D. CPU

Answer: B

Explanation:
Within IaaS, where the cloud customer is responsible for everything beyond the physical network, the number of users on a system would not be a factor in billing or service charges. The core cloud services for IaaS are based on the memory, storage, and CPU requirements of the cloud customer. Because the cloud customer with IaaS is responsible for its own images and deployments, these components comprise the basis of its cloud provisioning and measured services billing.

NEW QUESTION 225
- (Exam Topic 3)
Which data state would be most likely to use TLS as a protection mechanism?

A. Data in use
B. Data at rest
C. Archived
D. Data in transit

Answer: D

Explanation:
TLS would be used with data in transit, when packets are exchanged between clients or services and sent across a network. During the data-in-use state, the data is already protected via a technology such as TLS as it is exchanged over the network and then relies on other technologies such as digital signatures for protection while being used. The data-at-rest state primarily uses encryption for stored file objects. Archived data would be the same as data at rest.

NEW QUESTION 227
4 to 80.6 degrees Fahrenheit (or 18 to 27 degrees Celsius) as the optimal temperature range for data centers. None of these options is the recommendation from ASHRAE.

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 228
- (Exam Topic 3)
From a security perspective, what component of a cloud computing infrastructure represents the biggest concern?

A. Hypervisor
B. Management plane
C. Object storage
D. Encryption

Answer: B

Explanation:
The management plane will have broad administrative access to all host systems throughout an environment; as such, it represents the most pressing security concerns. A compromise of the management plane can directly lead to compromises of any other systems within the environment. Although hypervisors represent a significant security concern to an environment because their compromise would expose any virtual systems hosted within them, the management plane is a better choice in this case because it controls multiple hypervisors. Encryption and object storage both represent lower-level security concerns.

NEW QUESTION 233
- (Exam Topic 3)
Which of the following is not a risk management framework?

A. COBIT
B. Hex GBL
C. ISO 31000:2009
D. NIST SP 800-37

Answer: B

Explanation:
Hex GBL is a reference to a computer part in Terry Pratchett’s fictional Discworld universe. The rest are not.

NEW QUESTION 234
- (Exam Topic 3)
Which of the following threat types involves the sending of invalid and manipulated requests through a user's client to execute commands on the application under their own credentials?

A. Injection
B. Cross-site request forgery
C. Missing function-level access control
D. Cross-site scripting

Answer: B

Explanation:
A cross-site request forgery (CSRF) attack forces a client that a user has used to authenticate to an application to send forged requests under the user's own credentials to execute commands and requests that the application thinks are coming from a trusted client and user. Although this type of attack cannot be used to steal data directly because the attacker has no way to see the results of the commands, it does open other ways to compromise an application. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries.
Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes.

NEW QUESTION 238
- (Exam Topic 3)
One of the main components of system audits is the ability to track changes over time and to match these changes with continued compliance and internal processes.
Which aspect of cloud computing makes this particular component more challenging than in a traditional data center?

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

Answer: B

Explanation:
Cloud services make exclusive use of virtualization, and systems change over time, including the addition, subtraction, and reimaging of virtual machines. It is extremely unlikely that the exact same virtual machines and images used in a previous audit would still be in use or even available for a later audit, making the tracking of changes over time extremely difficult, or even impossible. Elasticity refers to the ability to add and remove resources from a system or service to meet current demand, and although it plays a factor in making the tracking of virtual machines very difficult over time, it is not the best answer in this case. Resource pooling pertains to a cloud environment sharing a large amount of resources between different customers and services. Portability refers to the ability to move systems or services easily between different cloud providers.

NEW QUESTION 239
- (Exam Topic 3)
Data center and operations design traditionally takes a tiered, topological approach.
Which of the following standards is focused on that approach and is prevalently used throughout the industry?

A. IDCA
B. NFPA
C. BICSI
D. Uptime Institute

Answer: D

Explanation:
The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers. The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The International Data Center Authority (IDCA) offers the Infinity Paradigm, which takes a macro-level approach to data center design.

NEW QUESTION 241
- (Exam Topic 3)
Digital investigations have adopted many of the same methodologies and protocols as other types of criminal or scientific inquiries.
What term pertains to the application of scientific norms and protocols to digital investigations?

A. Scientific
B. Investigative
C. Methodological
D. Forensics

Answer: D

Explanation:
Forensics refers to the application of scientific methods and protocols to the investigation of crimes. Although forensics has traditionally been applied to well-known criminal proceedings and investigations, the term equally applies to digital investigations and methods. Although the other answers provide similar-sounding terms and ideas, none is the appropriate answer in this case.

NEW QUESTION 244
- (Exam Topic 3)

ISO/IEC has established international standards for many aspects of computing and any processes or procedures related to information technology.
Which ISO/IEC standard has been established to provide a framework for handling eDiscovery processes?

A. ISO/IEC 27001
B. ISO/IEC 27002
C. ISO/IEC 27040
D. ISO/IEC 27050

Answer: D

Explanation:
ISO/IEC 27050 strives to establish an internationally accepted standard for eDiscovery processes and best practices. It encompasses all steps of the eDiscovery process, including the identification, preservation, collection, processing, review, analysis, and the final production of the requested data archive. ISO/IEC 27001 is a general security specification for an information security management system. ISO/IEC 27002 gives best practice recommendations for information security management. ISO/IEC 27040 is focused on the security of storage systems.

NEW QUESTION 246
- (Exam Topic 3)
Which of the following is NOT one of the main intended goals of a DLP solution?

A. Showing due diligence
B. Preventing malicious insiders
C. Regulatory compliance
D. Managing and minimizing risk

Answer: B

Explanation:
Data loss prevention (DLP) extends the capabilities for data protection beyond the standard and traditional security controls that are offered by operating systems, application containers, and network devices. DLP is not specifically implemented to counter malicious insiders, and would not be particularly effective in doing so, because a malicious insider with legitimate access would have other ways to obtain data. DLP is a set of practices and controls to manage and minimize risk, comply with regulatory requirements, and show due diligence with the protection of data.

NEW QUESTION 247
- (Exam Topic 3)
Which of the following tasks within a SaaS environment would NOT be something the cloud customer would be responsible for?

A. Authentication mechanism
B. Branding
C. Training
D. User access

Answer: A

Explanation:
The authentication mechanisms and implementations are the responsibility of the cloud provider because they are core components of the application platform and service. Within a SaaS implementation, the cloud
customer will provision user access, deploy branding to the application interface (typically), and provide or procure training for its users.

NEW QUESTION 252
- (Exam Topic 3)
Although the REST API supports a wide variety of data formats for communications and exchange, which data formats are the most commonly used?

A. SAML and HTML
B. XML and SAML
C. XML and JSON
D. JSON and SAML

Answer: C

Explanation:
JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API and are typically implemented with caching for increased scalability and performance. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data. HTML is used for authoring web pages for consumption by web browsers

NEW QUESTION 256
- (Exam Topic 3)
Which aspect of SaaS will alleviate much of the time and energy organizations spend on compliance (specifically baselines)?

A. Maintenance
B. Licensing
C. Standardization
D. Development

Answer: C

Explanation:

With the entire software platform being controlled by the cloud provider, the standardization of configurations and versioning is done automatically for the cloud customer. This alleviates the customer's need to track upgrades and releases for its own systems and development; instead, the onus is on the cloud provider. Although licensing is the responsibility of the cloud customer within SaaS, it does not have an impact on compliance requirements. Within SaaS, development and maintenance of the system are solely the responsibility of the cloud provider.

NEW QUESTION 257
- (Exam Topic 3)
Which cloud storage type resembles a virtual hard drive and can be utilized in the same manner and with the same type of features and capabilities?

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

Answer: A

Explanation:
Volume storage is allocated and mounted as a virtual hard drive within IaaS implementations, and it can be maintained and used the same way a traditional file system can. Object storage uses a flat structure on remote services that is accessed via opaque descriptors, structured storage resembles database storage, and unstructured storage is used to hold auxiliary files in conjunction with applications hosted within a PaaS implementation.

NEW QUESTION 261
- (Exam Topic 3)
With a federated identity system, where would a user perform their authentication when requesting services or application access?

A. Cloud provider
B. The application
C. Their home organization
D. Third-party authentication system

Answer: C

Explanation:
With a federated identity system, a user will perform authentication with their home organization, and the application will accept the authentication tokens and user information from the identity provider in order to grant access. The purpose of a federated system is to allow users to authenticate from their home organization. Therefore, using the application or a third-party authentication system would be contrary to the purpose of a federated system because it necessitates the creation of additional accounts. The use of a cloud provider would not be relevant to the operations of a federated system.

NEW QUESTION 265
- (Exam Topic 3)
Many aspects and features of cloud computing can make eDiscovery compliance more difficult or costly. Which aspect of cloud computing would be the MOST complicating factor?

A. Measured service
B. Broad network access
C. Multitenancy
D. Portability

Answer: C

Explanation:
With multitenancy, multiple customers share the same physical hardware and systems. With the nature of a cloud environment and how it writes data across diverse systems that are shared by others, the process of eDiscovery becomes much more complicated. Administrators cannot pull physical drives or easily isolate which data to capture. They not only have to focus on which data they need to collect, while ensuring they find all of it, but they also have to make sure that other data is not accidently collected and exposed along with it. Measured service is the aspect of a cloud where customers only pay for the services they are actually using, and for the duration of their use. Portability refers to the ease with which an application or service can be moved among different cloud providers. Broad network access refers to the nature of cloud services being accessed via the public Internet, either with or without secure tunneling technologies. None of these concepts would pertain to eDiscovery.

NEW QUESTION 266
- (Exam Topic 3)
Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?

A. Regulation
B. Multitenancy
C. Virtualization
D. Resource pooling

Answer: B

Explanation:
With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers. Especially within a public cloud model, it is not possible or practical for a cloud provider to alter its services for specific customer demands. Resource pooling and virtualization within a cloud environment would be the same for all customers, and would not impact certifications that a cloud provider might be willing to pursue. Regulations would form the basis for certification problems and would be a reason for a cloud provider to pursue specific certifications to meet customer requirements.

NEW QUESTION 268

- (Exam Topic 3)
In order to ensure ongoing compliance with regulatory requirements, which phase of the cloud data lifecycle must be tested regularly?

A. Archive
B. Share
C. Store
D. Destroy

Answer: A

Explanation:
In order to ensure compliance with regulations, it is important for an organization to regularly test the restorability of archived data. As technologies change and older systems are deprecated, the risk rises for an organization to lose the ability to restore data from the format in which it is stored. With the destroy, store, and share phases, the currently used technologies will be sufficient for an organization's needs in an ongoing basis, so the risk that is elevated with archived data is not present.

NEW QUESTION 272
- (Exam Topic 2)
Which of the following is NOT a domain of the Cloud Controls Matrix (CCM)?

A. Data center security
B. Human resources
C. Mobile security
D. Budgetary and cost controls

Answer: D

Explanation:
Budgetary and cost controls is not one of the domains outlined in the CCM.

NEW QUESTION 275
- (Exam Topic 2)
Which crucial aspect of cloud computing can be most threatened by insecure APIs?

A. Automation
B. Redundancy
C. Resource pooling
D. Elasticity

Answer: A

Explanation:
Cloud environments depend heavily on API calls for management and automation. Any vulnerability with the APIs can cause significant risk and exposure to all tenants of the cloud environment.

NEW QUESTION 280
- (Exam Topic 2)
What changes are necessary to application code in order to implement DNSSEC?

A. Adding encryption modules
B. Implementing certificate validations
C. Additional DNS lookups
D. No changes are needed.

Answer: D

Explanation:
To implement DNSSEC, no additional changes are needed to applications or their code because the integrity checks are all performed at the system level.

NEW QUESTION 284
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the oversight of processes and systems, as well as to ensuring their compliance with specific policies and regulations?

A. Governance
B. Regulatory requirements
C. Service-level agreements
D. Auditability

Answer: D

Explanation:
Auditing involves reports and evidence that show user activity, compliance with controls and regulations, the systems and processes that run and what they do, as well as information and data access and modification records. A cloud environment adds additional complexity to traditional audits because the cloud customer will not have the same level of access to systems and data as they would in a traditional data center.

NEW QUESTION 289

- (Exam Topic 2)
Which of the following is NOT a function performed by the handshake protocol of TLS?

A. Key exchange
B. Encryption
C. Negotiation of connection
D. Establish session ID

Answer: B

Explanation:
The handshake protocol negotiates and establishes the connection as well as handles the key exchange and establishes the session ID. It does not perform the actual encryption of data packets.

NEW QUESTION 294
- (Exam Topic 2)
Which aspect of cloud computing makes it very difficult to perform repeat audits over time to track changes and compliance?

A. Virtualization
B. Multitenancy
C. Resource pooling
D. Dynamic optimization

Answer: A

Explanation:
Cloud environments will regularly change virtual machines as patching and versions are changed. Unlike a physical environment, there is little continuity from one period of time to another. It is very unlikely that the same virtual machines would be in use during a repeat audit.

NEW QUESTION 297
- (Exam Topic 2)
Which type of audit report is considered a "restricted use" report for its intended audience?

A. SAS-70
B. SSAE-16
C. SOC Type 1
D. SOC Type 2

Answer: C

Explanation:
SOC Type 1 reports are considered "restricted use" reports. They are intended for management and stakeholders of an organization, clients of the service organization, and auditors of the organization. They are not intended for release beyond those audiences.

NEW QUESTION 301
- (Exam Topic 2)
Which process serves to prove the identity and credentials of a user requesting access to an application or data?

A. Repudiation
B. Authentication
C. Identification
D. Authorization

Answer: B

Explanation:
Authentication is the process of proving whether the identity presented by a user is true and valid. This can be done through common mechanisms such as user ID and password combinations or with more secure methods such as multifactor authentication.

NEW QUESTION 302
- (Exam Topic 2)
What does dynamic application security testing (DAST) NOT entail?

A. Scanning
B. Probing
C. Discovery
D. Knowledge of the system

Answer: D

Explanation:
Dynamic application security testing (DAST) is considered "black box" testing and begins with no inside knowledge of the application or its configurations. Everything about the application must be discovered during the testing.

NEW QUESTION 303
- (Exam Topic 2)
Which aspect of security is DNSSEC designed to ensure?

A. Integrity
B. Authentication
C. Availability
D. Confidentiality

Answer: A

Explanation:
DNSSEC is a security extension to the regular DNS protocol and services that allows for the validation of the integrity of DNS lookups. It does not address confidentiality or availability at all. It allows for a DNS client to perform DNS lookups and validate both their origin and authority via the cryptographic signature that accompanies the DNS response.

NEW QUESTION 305
- (Exam Topic 2)
Which security concept, if implemented correctly, will protect the data on a system, even if a malicious actor gains access to the actual system?

A. Sandboxing
B. Encryption
C. Firewalls
D. Access control

Answer: B

Explanation:
In any environment, data encryption is incredibly important to prevent unauthorized exposure of data either internally or externally. If a system is compromised by an attack, having the data encrypted on the system will prevent its unauthorized exposure or export, even with the system itself being exposed.

NEW QUESTION 310
- (Exam Topic 2)
Which value refers to the amount of time it takes to recover operations in a BCDR situation to meet management's objectives?

A. RSL
B. RPO
C. SRE
D. RTO

Answer: D

Explanation:
The recovery time objective (RTO) is a measure of the amount of time it would take to recover operations in the event of a disaster to the point where management's objectives are met for BCDR.

NEW QUESTION 312
- (Exam Topic 2)
Which approach is typically the most efficient method to use for data discovery?

A. Metadata
B. Content analysis
C. Labels
D. ACLs

Answer: A

Explanation:
Metadata is data about data. It contains information about the type of data, how it is stored and organized, or information about its creation and use.

NEW QUESTION 315
- (Exam Topic 2)
What is the biggest challenge to data discovery in a cloud environment?

A. Format
B. Ownership
C. Location
D. Multitenancy

Answer: C

Explanation:
With the distributed nature of cloud environments, the foremost challenge for data discovery is awareness of the location of data and keeping track of it during the constant motion of cloud storage systems.

NEW QUESTION 318
- (Exam Topic 2)
Which of the cloud deployment models requires the cloud customer to be part of a specific group or organization in order to host cloud services within it?

A. Community
B. Hybrid

C. Private
D. Public

Answer: A

Explanation:
A community cloud model is where customers that share a certain common bond or group membership come together to offer cloud services to their members, focused on common goals and interests.

NEW QUESTION 320
- (Exam Topic 2)
Which of the following is NOT an application or utility to apply and enforce baselines on a system?

A. Chef
B. GitHub
C. Puppet
D. Active Directory

Answer: B

Explanation:
GitHub is an application for code collaboration, including versioning and branching of code trees. It is not used for applying or maintaining system configurations.

NEW QUESTION 325
- (Exam Topic 2)
Which type of controls are the SOC Type 1 reports specifically focused on?

A. Integrity
B. PII
C. Financial
D. Privacy

Answer: C

Explanation:
SOC Type 1 reports are focused specifically on internal controls as they relate to financial reporting.

NEW QUESTION 329
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the assigning of jobs, tasks, and roles, as well as to ensuring they are successful and properly performed?

A. Service-level agreements
B. Governance
C. Regulatory requirements
D. Auditability

Answer: B

Explanation:
Governance at its core is the idea of assigning jobs, takes, roles, and responsibilities and ensuring they are satisfactory performed.

NEW QUESTION 330
- (Exam Topic 2)
What is an often overlooked concept that is essential to protecting the confidentiality of data?

A. Strong password
B. Training
C. Security controls
D. Policies

Answer: B

Explanation:
While the main focus of confidentiality revolves around technological requirements or particular security methods, an important and often overlooked aspect of safeguarding data confidentiality is appropriate and comprehensive training for those with access to it. Training should be focused on the safe handling of sensitive information overall, including best practices for network activities as well as physical security of the devices or workstations used to access the application.

NEW QUESTION 335
- (Exam Topic 2)
What type of masking strategy involves replacing data on a system while it passes between the data and application layers?

A. Dynamic
B. Static
C. Replication
D. Duplication

Answer: A

Explanation:
With dynamic masking, production environments are protected with the masking process being implemented between the application and data layers of the application. This allows for a masking translation to take place live in the system and during normal application processing of data.

NEW QUESTION 338
- (Exam Topic 2)
Which of the following service capabilities gives the cloud customer the most control over resources and configurations?

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

Answer: C

Explanation:
The infrastructure service capability gives the cloud customer substantial control in provisioning and configuring resources, including processing, storage, and network resources.

NEW QUESTION 343
- (Exam Topic 2)
Which aspect of cloud computing would make the use of a cloud the most attractive as a BCDR solution?

A. Interoperability
B. Resource pooling
C. Portability
D. Measured service

Answer: D

Explanation:
Measured service means that costs are only incurred when a cloud customer is actually using cloud services. This is ideal for a business continuity and disaster recovery (BCDR) solution because it negates the need to keep hardware or resources on standby in case of a disaster. Services can be initiated when needed and without costs unless needed.

NEW QUESTION 344
- (Exam Topic 2)
At which stage of the BCDR plan creation phase should security be included in discussions?

A. Define scope
B. Analyze
C. Assess risk
D. Gather requirements

Answer: A

Explanation:
Security should be included in discussions from the very first phase when defining the scope. Adding security later is likely to incur additional costs in time and money, or will result in an incomplete or inadequate plan.

NEW QUESTION 347
- (Exam Topic 2)
What type of data does data rights management (DRM) protect?

A. Consumer
B. PII
C. Financial
D. Healthcare

Answer: A

Explanation:
DRM applies to the protection of consumer media, such as music, publications, video, movies, and soon.

NEW QUESTION 351
- (Exam Topic 2)
Which of the following can be useful for protecting cloud customers from a denial-of-service (DoS) attack against another customer hosted in the same cloud?

A. Reservations
B. Measured service
C. Limits
D. Shares

Answer: A

Explanation:
Reservations ensure that a minimum level of resources will always be available to a cloud customer for them to start and operate their services. In the event of a

DoS attack against one customer, they can guarantee that the other customers will still be able to operate.

NEW QUESTION 353
- (Exam Topic 2)
Which of the cloud deployment models offers the most control and input to the cloud customer as to how the overall cloud environment is implemented and configured?

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

Answer: D

Explanation:
A private cloud model, and the specific contractual relationships involved, will give a cloud customer the most level of input and control over how the overall cloud environment is designed and implemented. This would be even more so in cases where the private cloud is owned and operated by the same organization that is hosting services within it.

NEW QUESTION 357
- (Exam Topic 2)
Which of the following should NOT be part of the requirement analysis phase of the software development lifecycle?

A. Functionality
B. Programming languages
C. Software platform
D. Security requirements

Answer: D

Explanation:
Security requirements should be incorporated into the software development lifecycle (SDLC) from the earliest requirement gathering stage and should be incorporated prior to the requirement analysis phase.

NEW QUESTION 358
- (Exam Topic 2)
What does static application security testing (SAST) offer as a tool to the testers?

A. Production system scanning
B. Injection attempts
C. Source code access
D. Live testing

Answer: C

Explanation:
Static application security testing (SAST) is conducted with knowledge of the system, including source code, and is done against offline systems.

NEW QUESTION 360
- (Exam Topic 2)
What must SOAP rely on for security?

A. Encryption
B. Tokenization
C. TLS
D. SSL

Answer: A

Explanation:
Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for passing data, and it must rely on the encryption of those data packages for security.

NEW QUESTION 361
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the ability to reuse or move components of an application or service?

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

Answer: B

Explanation:
Interoperability is the ease with which one can move or reuse components of an application or service. This is maximized when services are designed without specific dependencies on underlying platforms, operating systems, locations, or cloud providers.

NEW QUESTION 366
- (Exam Topic 2)
Who would be responsible for implementing IPsec to secure communications for an application?

A. Developers
B. Systems staff
C. Auditors
D. Cloud customer

Answer: B

Explanation:
Because IPsec is implemented at the system or network level, it is the responsibility of the systems staff. IPsec removes the responsibility from developers, whereas other technologies such as TLS would be implemented by developers.

NEW QUESTION 369
- (Exam Topic 2)
Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?

A. Six months
B. One month
C. One year
D. One week

Answer: A

Explanation:
SOC Type 2 reports are focused on the same policies and procedures, as well as their effectiveness, as SOC Type 1 reports, but are evaluated over a period of at least six consecutive months, rather than a finite point in time.

NEW QUESTION 372
- (Exam Topic 2)
Which of the following is NOT a focus or consideration of an internal audit?

A. Certification
B. Design
C. Costs
D. Operational efficiency

Answer: A

Explanation:
In order to obtain and comply with certifications, independent external audits must be performed and satisfied. Although some testing of certification controls can be part of an internal audit, they will not satisfy requirements.

NEW QUESTION 376
- (Exam Topic 1)
Which of the following roles is responsible for creating cloud components and the testing and validation of services?

A. Cloud auditor
B. Inter-cloud provider
C. Cloud service broker
D. Cloud service developer

Answer: D

Explanation:
The cloud service developer is responsible for developing and creating cloud components and services, as well as for testing and validating services.

NEW QUESTION 381
- (Exam Topic 1)
Which of the following would NOT be considered part of resource pooling with an Infrastructure as a Service implementation?

A. Storage
B. Application
C. Mamory
D. CPU

Answer: B

Explanation:
Infrastructure as a Service pools the compute resources for platforms and applications to build upon, including CPU, memory, and storage. Applications are not part of an IaaS offering from the cloud provider.

NEW QUESTION 383

- (Exam Topic 1)
When is a virtual machine susceptible to attacks while a physical server in the same state would not be?

A. When it is behind a WAF
B. When it is behind an IPS
C. When it is not patched
D. When it is powered off

Answer: D

Explanation:
A virtual machine is ultimately an image file residing a file system. Because of this, even when a virtual machine is "powered off," it is still susceptible to attacks and modification. A physical server that is powered off would not be susceptible to attacks.

NEW QUESTION 384
- (Exam Topic 1)
What is the first stage of the cloud data lifecycle where security controls can be implemented?

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

Answer: B

Explanation:
The "store" phase of the cloud data lifecycle, which typically occurs simultaneously with the "create" phase, or immediately thereafter, is the first phase where security controls can be implemented. In most case, the manner in which the data is stored will be based on its classification.

NEW QUESTION 388
- (Exam Topic 1)
Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?

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

Answer: B

Explanation:
Popular services such as iCloud, Dropbox, and OneDrive are all publicly available and are open to any user for free, with possible add-on services offered for a cost.

NEW QUESTION 389
- (Exam Topic 1)
Which protocol allows a system to use block-level storage as if it was a SAN, but over TCP network traffic instead?

A. SATA
B. iSCSI
C. TLS
D. SCSI

Answer: B

Explanation:
iSCSI is a protocol that allows for the transmission and use of SCSI commands and features over a TCP-based network. iSCSI allows systems to use block-level storage that looks and behaves as a SAN would with physical servers, but to leverage the TCP network within a virtualized environment and cloud.

NEW QUESTION 391
- (Exam Topic 1)
What is the biggest negative to leasing space in a data center versus building or maintain your own?

A. Costs
B. Control
C. Certification
D. Regulation

Answer: B

Explanation:
When leasing space in a data center, an organization will give up a large degree of control as to how it is built and maintained, and instead must conform to the policies and procedures of the owners and operators of the data center.

NEW QUESTION 392
- (Exam Topic 1)
Which of the following is the optimal humidity level for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air

Conditioning Engineers (ASHRAE)?

A. 30-50 percent relative humidity
B. 50-75 percent relative humidity
C. 20-40 percent relative humidity
D. 40-60 percent relative humidity

Answer: D

Explanation:
The guidelines from ASHRAE establish 40-60 percent relative humidity as optimal for a data center.

NEW QUESTION 393
- (Exam Topic 1)
If you're using iSCSI in a cloud environment, what must come from an external protocol or application?

A. Kerberos support
B. CHAP support
C. Authentication
D. Encryption

Answer: D

Explanation:
iSCSI does not natively support encryption, so another technology such as IPsec must be used to encrypt communications.

NEW QUESTION 398
- (Exam Topic 1)
Which of the following threat types can occur when baselines are not appropriately applied or unauthorized changes are made?

A. Insecure direct object references
B. Unvalidated redirects and forwards
C. Security misconfiguration
D. Sensitive data exposure

Answer: C

Explanation:
Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner. This can be caused from a shortcoming in security baselines or configurations, unauthorized changes to system configurations, or a failure to patch and upgrade systems as the vendor releases security patches.

NEW QUESTION 403
- (Exam Topic 1)
Which of the following statements accurately describes VLANs?

A. They are not restricted to the same data center or the same racks.
B. They are not restricted to the name rack but restricted to the same data center.
C. They are restricted to the same racks and data centers.
D. They are not restricted to the same rack but restricted to same switches.

Answer: A

Explanation:
A virtual area network (VLAN) can span any networks within a data center, or it can span across different physical locations and data centers.

NEW QUESTION 404
- (Exam Topic 1)
Which of the following roles is responsible for preparing systems for the cloud, administering and monitoring services, and managing inventory and assets?

A. Cloud service business manager
B. Cloud service deployment manager
C. Cloud service operations manager
D. Cloud service manager

Answer: C

Explanation:
The cloud service operations manager is responsible for preparing systems for the cloud, administering and monitoring services, providing audit data as requested or required, and managing inventory and assets.

NEW QUESTION 408
- (Exam Topic 1)
Which technology is NOT commonly used for security with data in transit?

A. DNSSEC
B. IPsec

C. VPN
D. HTTPS

Answer: A

Explanation:
DNSSEC relates to the integrity of DNS resolutions and the prevention of spoofing or redirection, and does not pertain to the actual security of transmissions or the protection of data.

NEW QUESTION 411
- (Exam Topic 1)
Which of the following does NOT relate to the hiding of sensitive data from data sets?

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

Answer: B

Explanation:
Federation pertains to authenticating systems between different organizations.

NEW QUESTION 416
- (Exam Topic 1)
Which aspect of cloud computing will be most negatively impacted by vendor lock-in?

A. Elasticity
B. Reversibility
C. Interoperability
D. Portability

Answer: D

Explanation:
A cloud customer utilizing proprietary APIs or services from one cloud provider that are unlikely to be available from another cloud provider will most negatively impact portability.

NEW QUESTION 418
- (Exam Topic 1)
Which of the following roles involves overseeing billing, purchasing, and requesting audit reports for an organization within a cloud environment?

A. Cloud service user
B. Cloud service business manager
C. Cloud service administrator
D. Cloud service integrator

Answer: B

Explanation:
The cloud service business manager is responsible for overseeing business and billing administration, purchasing cloud services, and requesting audit reports when necessary

NEW QUESTION 423
- (Exam Topic 1)
Which type of cloud model typically presents the most challenges to a cloud customer during the "destroy" phase of the cloud data lifecycle?

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

Answer: C

Explanation:
With many SaaS implementations, data is not isolated to a particular customer but rather is part of the overall application. When it comes to data destruction, a particular challenge is ensuring that all of a customer's data is completely destroyed while not impacting the data of other customers.

NEW QUESTION 425
- (Exam Topic 1)
Which of the following roles is responsible for gathering metrics on cloud services and managing cloud deployments and the deployment processes?

A. Cloud service business manager
B. Cloud service operations manager
C. Cloud service manager
D. Cloud service deployment manager

Answer: D

Explanation:
The cloud service deployment manager is responsible for gathering metrics on cloud services, managing cloud deployments and the deployment process, and defining the environments and processes.

NEW QUESTION 429
- (Exam Topic 1)
Which of the following would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?

A. Resource pooling
B. Virtualization
C. Multitenancy
D. Regulation

Answer: C

Explanation:
With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers, and especially within a public cloud model, it is not possible or practical for a cloud provider to alter their services for specific customer demands.

NEW QUESTION 430
- (Exam Topic 1)
What is a serious complication an organization faces from the perspective of compliance with international operations?

A. Different certifications
B. Multiple jurisdictions
C. Different capabilities
D. Different operational procedures

Answer: B

Explanation:
When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, and many times they might be in contention with one other or not clearly applicable. These requirements can include the location of the users and the type of data they enter into systems, the laws governing the organization that owns the application and any regulatory requirements they may have, as well as the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which might be multiple jurisdictions as well.

NEW QUESTION 435
- (Exam Topic 1)
Which of the following roles involves the provisioning and delivery of cloud services?

A. Cloud service deployment manager
B. Cloud service business manager
C. Cloud service manager
D. Cloud service operations manager

Answer: C

Explanation:
The cloud service manager is responsible for the delivery of cloud services, the provisioning of cloud services, and the overall management of cloud services.

NEW QUESTION 439
- (Exam Topic 1)
Which protocol does the REST API depend on?

A. HTTP
B. XML
C. SAML
D. SSH

Answer: A

Explanation:
Representational State Transfer (REST) is a software architectural scheme that applies the components, connectors, and data conduits for many web applications used on the Internet. It uses and relies on the HTTP protocol and supports a variety of data formats.

NEW QUESTION 440
- (Exam Topic 1)
Which is the appropriate phase of the cloud data lifecycle for determining the data's classification?

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

Answer: A

Explanation:
Any time data is created, modified, or imported, the classification needs to be evaluated and set from the earliest phase to ensure security is always properly maintained for the duration of its lifecycle.

NEW QUESTION 443
- (Exam Topic 1)
Which data formats are most commonly used with the REST API?

A. JSON and SAML
B. XML and SAML
C. XML and JSON
D. SAML and HTML

Answer: C

Explanation:
JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API, and are typically implemented with caching for increased scalability and performance.

NEW QUESTION 448
- (Exam Topic 1)
Which of the following are the storage types associated with IaaS?

A. Volume and object
B. Volume and label
C. Volume and container
D. Object and target

Answer: A

NEW QUESTION 449
- (Exam Topic 1)
What is used for local, physical access to hardware within a data center?

A. SSH
B. KVM
C. VPN
D. RDP

Answer: B

Explanation:
Local, physical access in a data center is done via KVM (keyboard, video, mouse) switches.

NEW QUESTION 450
- (Exam Topic 1)
What must be secured on physical hardware to prevent unauthorized access to systems?

A. BIOS
B. SSH
C. RDP
D. ALOM

Answer: A

Explanation:
BIOS is the firmware that governs the physical initiation and boot up of a piece of hardware. If it is compromised, an attacker could have access to hosted systems and make configurations changes to expose or disable some security elements on the system.

NEW QUESTION 452
.....

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/