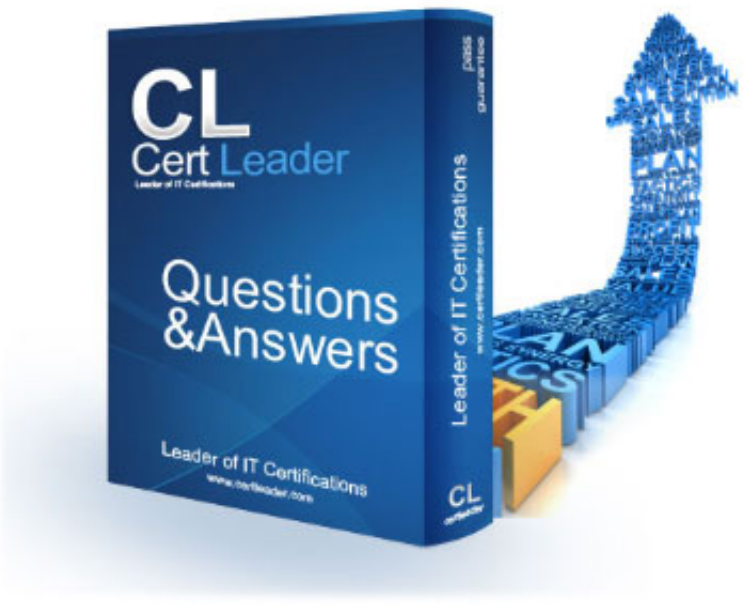
CCSP Dumps

Certified Cloud Security Professional

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



NEW QUESTION 1
- (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 2
- (Exam Topic 4)
Which of the following areas of responsibility always falls completely under the purview of the cloud provider, regardless of which cloud service category is used?

A. Infrastructure
B. Data
C. Physical
D. Governance

Answer: C

Explanation:
Regardless of the cloud service category used, the physical environment is always the sole responsibility of the cloud provider. In many instances, the cloud provider will supply audit reports or some general information about their physical security practices, especially to those customers or potential customers that may have regulatory requirements, but otherwise the cloud customer will have very little insight into the physical environment. With IaaS, the infrastructure is a shared responsibility between the cloud provider and cloud customer. With all cloud service categories, the data and governance are always the sole responsibility of the cloud customer.

NEW QUESTION 3
- (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 4
- (Exam Topic 4)
In which cloud service model is the customer required to maintain the OS?

A. Iaas
B. CaaS
C. PaaS
D. SaaS

Answer: A

Explanation:
In IaaS, the service is bare metal, and the customer has to install the OS and the software; the customer then is responsible for maintaining that OS. In the other models, the provider installs and maintains the OS.

NEW QUESTION 5
- (Exam Topic 4)
What is the intellectual property protection for a confidential recipe for muffins?

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

Answer: C

Explanation:
Confidential recipes unique to the organization are trade secrets. The other answers listed are answers to other questions.

NEW QUESTION 6
- (Exam Topic 4)
When data discovery is undertaken, three main approaches or strategies are commonly used to determine what the type of data, its format, and composition are for the purposes of classification.
Which of the following is NOT one of the three main approaches to data discovery?

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

Answer: B

Explanation:
Hashing involves taking a block of data and, through the use of a one-way operation, producing a fixed-size value that can be used for comparison with other data. It is used primarily for protecting data and allowing for rapid comparison when matching data values such as passwords. Labels involve looking for header information or other categorizations of data to determine its type and possible classifications. Metadata involves looking at information attributes of the data, such as creator, application, type, and so on, in determining classification. Content analysis involves examining the actual data itself for its composition and classification level.

NEW QUESTION 7
- (Exam Topic 4)
Which ITIL component is an ongoing, iterative process of tracking all deployed and configured resources that an organization uses and depends on, whether they are hosted in a traditional data center or a cloud?

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

Answer: D

Explanation:
Configuration management tracks and maintains detailed information about all IT components within an organization. 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. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

NEW QUESTION 8
- (Exam Topic 4)
Which of the following concepts is NOT one of the core components to an encryption system architecture?

A. Software
B. Network
C. Keys
D. Data

Answer: B

Explanation:
The network utilized is not one of the key components of an encryption system architecture. In fact, a network is not even required for encryption systems or the processing and protection of data. The data, software used for the encryption engine itself, and the keys used to implement the encryption are all core components of an encryption system architecture.

NEW QUESTION 9
- (Exam Topic 4)
The most pragmatic option for data disposal in the cloud is which of the following?

A. Cryptoshredding
B. Overwriting
C. Cold fusion
D. Melting

Answer: A

Explanation:
We don’t have physical ownership, control, or even access to the devices holding the data, so physical destruction, including melting, is not an option. Overwriting is a possibility, but it is complicated by the difficulty of locating all the sectors and storage areas that might have contained our data, and by the likelihood that constant backups in the cloud increase the chance we’ll miss something as it’s being overwritten. Cryptoshredding is the only reasonable alternative. Cold fusion is a red herring.

NEW QUESTION 10
- (Exam Topic 4)
Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like:

A. Ransomware
B. Syn floods
C. XSS and SQL injection
D. Password cracking

Answer: C

Explanation:
WAFs detect how the application interacts with the environment, so they are optimal for detecting and refuting things like SQL injection and XSS. Password cracking, syn floods, and ransomware usually aren't taking place in the same way as injection and XSS, and they are better addressed with controls at the router and through the use of HIDS, NIDS, and antimalware tools.

NEW QUESTION 10
- (Exam Topic 4)
Which of the following is not a way to manage risk?

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

Answer: D

Explanation:
Enveloping is a nonsense term, unrelated to risk management. The rest are not.

NEW QUESTION 11
- (Exam Topic 4)
Which of the following provides assurance, to a predetermined acceptable level of certainty, that an entity is indeed who they claim to be?

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

Answer: A

Explanation:
Authentication goes a step further than identification by providing a means for proving an entity's identification. Authentication is most commonly done through mechanisms such as passwords. Identification involves ascertaining who the entity is, but without a means of proving it, such as a name or user ID. Authorization occurs after authentication and sets access permissions and other privileges within a system or application for the user. Proofing is not a term that is relevant to the question.

NEW QUESTION 12
- (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 14
- (Exam Topic 4)
As part of the auditing process, getting a report on the deviations between intended configurations and actual policy is often crucial for an organization.
What term pertains to the process of generating such a report?

A. Deficiencies
B. Findings
C. Gap analysis
D. Errors

Answer: C

Explanation:
The gap analysis determines if there are any differences between the actual configurations in use on systems and the policies that govern what the configurations are expected or mandated to be. The other terms provided are all similar to the correct answer ("findings" in particular is often used to articulate deviations in configurations), but gap analysis is the official term used.

NEW QUESTION 15
- (Exam Topic 4)

Cryptographic keys for encrypted data stored in the cloud should be _____.

A. Not stored with the cloud provider.
B. Generated with redundancy
C. At least 128 bits long
D. Split into groups

Answer: A

Explanation:
Cryptographic keys should not be stored along with the data they secure, regardless of key length. We don't split crypto keys or generate redundant keys (doing so would violate the principle of secrecy necessary for keys to serve their purpose).

NEW QUESTION 19
- (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 21
- (Exam Topic 4)
What is the Cloud Security Alliance Cloud Controls Matrix (CCM)?

A. A set of software development life cycle requirements for cloud service providers
B. An inventory of cloud services security controls that are arranged into a hierarchy of security domains
C. An inventory of cloud service security controls that are arranged into separate security domains
D. A set of regulatory requirements for cloud service providers

Answer: C

Explanation:
The CSA CCM is an inventory of cloud service security controls that are arranged into separate security domains, not a hierarchy.

NEW QUESTION 25
- (Exam Topic 4)
Which of the following is NOT a component of access control?

A. Accounting
B. Federation
C. Authorization
D. Authentication

Answer: B

Explanation:
Federation is not a component of access control. Instead, it is used to allow users possessing credentials from other authorities and systems to access services outside of their domain. This allows for access and trust without the need to create additional, local credentials. Access control encompasses not only the key concepts of authorization and authentication, but also accounting. Accounting consists of collecting and maintaining logs for both authentication and authorization for operational and regulatory requirements.

NEW QUESTION 26
- (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 27
- (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 30
- (Exam Topic 4)
DLP solutions can aid in deterring loss due to which of the following?

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

Answer: A

Explanation:
DLP solutions may protect against inadvertent disclosure. Randomization is a technique for obscuring data, not a risk to data. DLP tools will not protect against risks from natural disasters, or against impacts due to device failure.

NEW QUESTION 33
- (Exam Topic 4)
What type of solution is at the core of virtually all directory services?

A. WS
B. LDAP
C. ADFS
D. PKI

Answer: B

Explanation:
The Lightweight Directory Access Protocol (LDAP) forms the basis of virtually all directory services, regardless of the specific vendor or software package.WS is a protocol for information exchange between two systems and does not actually store the data. ADFS is a Windows component for enabling single sign-on for the operating system and applications, but it relies on data from an LDAP server. PKI is used for managing and issuing security certificates.

NEW QUESTION 38
- (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 43
- (Exam Topic 4)
Which of the following best describes SAML?

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

Answer: D

NEW QUESTION 47
- (Exam Topic 4)
The WS-Security standards are built around all of the following standards except which one?

A. SAML

B. WDSL
C. XML
D. SOAP

Answer: A

Explanation:
The WS-Security specifications, as well as the WS-Federation system, are built upon XML, WDSL, and SOAP. SAML is a very similar protocol that is used as an alternative to WS.XML, WDSL, and SOAP are all integral to the WS-Security specifications.

NEW QUESTION 50
- (Exam Topic 4)
Database activity monitoring (DAM) can be:

A. Host-based or network-based
B. Server-based or client-based
C. Used in the place of encryption
D. Used in place of data masking

Answer: A

Explanation:
We don’t use DAM in place of encryption or masking; DAM augments these options without replacing them. We don’t usually think of the database interaction as client-server, so A is the best answer.

NEW QUESTION 53
- (Exam Topic 4)
Which of the following technologies is NOT commonly used for accessing systems and services in a cloud environment in a secure manner?

A. KVM
B. HTTPS
C. VPN
D. TLS

Answer: A

Explanation:
A keyboard-video-mouse (KVM) system is commonly used for directly accessing server terminals in a data center. It is not a method that would be possible within a cloud environment, primarily due to the use virtualized systems, but also because only the cloud provider's staff would be allowed the physical access to hardware systems that's provided by a KVM. Hypertext Transfer Protocol Secure (HTTPS), virtual private network (VPN), and Transport Layer Security (TLS) are all technologies and protocols that are widely used with cloud implementations for secure access to systems and services.

NEW QUESTION 55
- (Exam Topic 4)
DLP solutions can aid in deterring loss due to which of the following?

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

Answer: C

Explanation:
DLP solutions may protect against inadvertent disclosure. Randomization is a technique for obscuring data, not a risk to data. DLP tools will not protect against risks from natural disasters, or against impacts due to device failure.

NEW QUESTION 57
- (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 58
- (Exam Topic 4)
The different cloud service models have varying levels of responsibilities for functions and operations depending with the model's level of service.

In which of the following models would the responsibility for patching lie predominantly with the cloud customer?

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

Answer: D

Explanation:
With Infrastructure as a Service (IaaS), the cloud customer is responsible for deploying and maintaining its own systems and virtual machines. Therefore, the customer is solely responsible for patching and any other security updates it finds necessary. With Software as a Service (SaaS), Platform as a Service (PaaS), and Desktop as a Service (DaaS), the cloud provider maintains the infrastructure components and is responsible for maintaining and patching them.

NEW QUESTION 61
- (Exam Topic 4)
What does static application security testing (SAST) offer as a tool to the testers that makes it unique compared to other common security testing methodologies?

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

Answer: B

Explanation:
Static application security testing (SAST) is conducted against offline systems with previous knowledge of them, including their source code. Live testing is not part of static testing but rather is associated with dynamic testing. Production system scanning is not appropriate because static testing is done against offline systems. Injection attempts are done with many different types of testing and are not unique to one particular type. It is therefore not the best answer to the question.

NEW QUESTION 62
- (Exam Topic 4)
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:

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

Answer: C

Explanation:
Data discovery is a term used to describe the process of identifying information according to specific traits or categories. The rest are all methods for obscuring data.

NEW QUESTION 63
- (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 64
- (Exam Topic 4)
The GAPP framework was developed through a joint effort between the major Canadian and American
professional accounting associations in order to assist their members with managing and preventing risks to the privacy of their data and customers.
Which of the following is the meaning of GAPP?

A. General accounting personal privacy
B. Generally accepted privacy practices
C. Generally accepted privacy principles
D. General accounting privacy policies

Answer: C

NEW QUESTION 67
- (Exam Topic 4)
What masking strategy involves the replacing of sensitive data at the time it is accessed and used as it flows between the data and application layers of a service?

A. Active

B. Static
C. Dynamic
D. Transactional

Answer: C

Explanation:
Dynamic masking involves the live replacing of sensitive data fields during transactional use between the data and application layers of a service. Static masking involves creating a full data set with the sensitive data fields masked, but is not done during live transactions like dynamic masking. Active and transactional are offered as similar types of answers but are not types of masking.

NEW QUESTION 69
- (Exam Topic 4)
Which of the following report is most aligned with financial control audits?

A. SSAE 16
B. SOC 2
C. SOC 1
D. SOC 3

Answer: C

Explanation:
The SOC 1 report focuses primarily on controls associated with financial services. While IT controls are certainly part of most accounting systems today, the focus is on the controls around those financial systems.

NEW QUESTION 73
- (Exam Topic 4)
The baseline should cover which of the following?

A. Data breach alerting and reporting
B. All regulatory compliance requirements
C. As many systems throughout the organization as possible
D. A process for version control

Answer: C

Explanation:
The more systems that be included in the baseline, the more cost-effective and scalable the baseline is. The baseline does not deal with breaches or version control; those are the provinces of the security office and CMB, respectively. Regulatory compliance might (and usually will) go beyond the baseline and involve systems, processes, and personnel that are not subject to the baseline.

NEW QUESTION 78
- (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 79
- (Exam Topic 4)
When a system needs to be exposed to the public Internet, what type of secure system would be used to perform only the desired operations?

A. Firewall
B. Proxy
C. Honeypot
D. Bastion

Answer: D

Explanation:
A bastion is a system that is exposed to the public Internet to perform a specific function, but it is highly restricted and secured to just that function. Any nonessential services and access are removed from the bastion so that security countermeasures and monitoring can be focused just on the bastion's specific duties. A honeypot is a system designed to look like a production system to entice attackers, but it does not contain any real data. It is used for learning about types of attacks and enabling countermeasures for them. A firewall is used within a network to limit access between IP addresses and ports. A proxy server provides additional security to and rulesets for network traffic that is allowed to pass through it to a service destination.

NEW QUESTION 83
- (Exam Topic 4)

Which protocol, as a part of TLS, handles negotiating and establishing a connection between two parties?

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

Answer: D

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

NEW QUESTION 86
- (Exam Topic 4)
Apart from using encryption at the file system level, what technology is the most widely used to protect data stored in an object storage system?

A. TLS
B. HTTPS
C. VPN
D. IRM

Answer: D

Explanation:
Information rights management (IRM) technologies allow security controls and policies to be enforced on a data object regardless of where it resides. They also allow for extended controls such as expirations and copying restrictions, which are not available through traditional control mechanisms. Hypertext Transfer Protocol Secure (HTTPS), virtual private network (VPN), and Transport Layer Security (TLS) are all technologies and protocols that are widely used with cloud implementations for secure access to systems and services and likely will be used in conjunction with other object data protection strategies.

NEW QUESTION 87
- (Exam Topic 4)
Key maintenance and security are paramount within a cloud environment due to the widespread use of encryption for both data and transmissions.
Which of the following key-management systems would provide the most robust control over and ownership of the key-management processes for the cloud customer?

A. Remote key management service
B. Local key management service
C. Client key management service
D. Internal key management service

Answer: A

Explanation:
A remote key management system resides away from the cloud environment and is owned and controlled by the cloud customer. With the use of a remote service, the cloud customer can avoid being locked into a proprietary system from the cloud provider, but also must ensure that service is compatible with the services offered by the cloud provider. A local key management system resides on the actual servers using the keys, which does not provide optimal security or control over them. Both the terms internal key management service and client key management service are provided as distractors.

NEW QUESTION 88
- (Exam Topic 4)
What concept and operational process must be spelled out clearly, as far as roles and responsibilities go, between the cloud provider and cloud customer for the mitigation of any problems or security events?

A. Incident response
B. Problem management
C. Change management
D. Conflict response

Answer: A

Explanation:
Incident response is the process through which security or operational issues are handled, including and coordination with and communication to the appropriate stakeholders. None of the other terms provided is the correct response.

NEW QUESTION 91
- (Exam Topic 4)
Which of the following areas of responsibility would be shared between the cloud customer and cloud provider within the Software as a Service (SaaS) category?

A. Data
B. Governance
C. Application
D. Physical

Answer: C

Explanation:

With SaaS, the application is a shared responsibility between the cloud provider and cloud customer. Although the cloud provider is responsible for deploying, maintaining, and securing the application, the cloud customer does carry some responsibility for the configuration of users and options. Regardless of the cloud service category used, the physical environment is always the sole responsibility of the cloud provider. With all cloud service categories, the data and governance are always the sole responsibility of the cloud customer.

NEW QUESTION 94
- (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 98
- (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 100
- (Exam Topic 4)
Identity and access management (IAM) is a security discipline that ensures which of the following?

A. That all users are properly authorized
B. That the right individual gets access to the right resources at the right time for the right reasons.
C. That all users are properly authenticated
D. That unauthorized users will get access to the right resources at the right time for the right reasons

Answer: B

Explanation:
Options A and C are also correct, but included in B, making B the best choice. D is incorrect, because we don't want unauthorized users gaining access.

NEW QUESTION 102
- (Exam Topic 4)
All of these are methods of data discovery, except:

A. Label-based
B. User-based
C. Content-based
D. Metadata-based

Answer: B

Explanation:
All the others are valid methods of data discovery; user-based is a red herring with no meaning.

NEW QUESTION 103
- (Exam Topic 4)
Upon completing a risk analysis, a company has four different approaches to addressing risk. Which approach it takes will be based on costs, available options, and adherence to any regulatory requirements from independent audits.
Which of the following groupings correctly represents the four possible approaches?

A. Accept, avoid, transfer, mitigate
B. Accept, deny, transfer, mitigate
C. Accept, deny, mitigate, revise
D. Accept, dismiss, transfer, mitigate

Answer: A

Explanation:
The four possible approaches to risk are as follows: accept (do not patch and continue with the risk), avoid (implement solutions to prevent the risk from occurring),

transfer (take out insurance), and mitigate (change configurations or patch to resolve the risk). Each of these answers contains at least one incorrect approach name.

NEW QUESTION 107
- (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 109
- (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 111
- (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 112
- (Exam Topic 4)
A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence.
Which core concept of cloud computing is most related to vendor lock-in?

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

Answer: C

Explanation:
Portability is the ability for a cloud customer to easily move their systems, services, and applications among different cloud providers. By avoiding reliance on proprietary APIs and other vendor-specific cloud features, an organization can maintain flexibility to move among the various cloud providers with greater ease. Reversibility refers to the ability for a cloud customer to quickly and easy remove all their services and data from a cloud provider. Interoperability is the ability to reuse services and components for other applications and uses. Scalability refers to the ability of a cloud environment to add or remove resources to meet current demands.

NEW QUESTION 115
- (Exam Topic 4)

Maintenance mode requires all of these actions except:

A. Remove all active production instances
B. Ensure logging continues
C. Initiate enhanced security controls
D. Prevent new logins

Answer: C

Explanation:
While the other answers are all steps in moving from normal operations to maintenance mode, we do not necessarily initiate any enhanced security controls.

NEW QUESTION 117
- (Exam Topic 4)
User access to the cloud environment can be administered in all of the following ways except:

A. Provider provides administration on behalf the customer
B. Customer directly administers access
C. Third party provides administration on behalf of the customer
D. Customer provides administration on behalf of the provider

Answer: D

Explanation:
The customer does not administer on behalf of the provider. All the rest are possible options.

NEW QUESTION 121
- (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 124
- (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 129
- (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 134
- (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 138
- (Exam Topic 4)
To address shared monitoring and testing responsibilities in a cloud configuration, the provider might offer all these to the cloud customer except:

A. Access to audit logs and performance data
B. DLP solution results
C. Security control administration
D. SIM, SEI
E. and SEM logs

Answer: C

Explanation:
While the provider might share any of the other options listed, the provider will not share administration of security controls with the customer. Security controls are the sole province of the provider.

NEW QUESTION 139
- (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 141
- (Exam Topic 4)
What is the term we use to describe the general ease and efficiency of moving data from one cloud provider either to another cloud provider or down from the cloud?

A. Obfuscation
B. Elasticity
C. Mobility
D. Portability

Answer: D

Explanation:
Elasticity is the name for the benefit of cloud computing where resources can be apportioned as necessary to meet customer demand. Obfuscation is a technique to hide full raw datasets, either from personnel who do not have need to know or for use in testing. Mobility is not a term pertinent to the CBK.

NEW QUESTION 143
- (Exam Topic 4)
Countermeasures for protecting cloud operations against internal threats include all of the following except:

A. Mandatory vacation
B. Least privilege
C. Separation of duties
D. Conflict of interest

Answer: D

Explanation:
Conflict of interest is a threat, not a control.

NEW QUESTION 146
- (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 150
- (Exam Topic 4)
Your IT steering committee has, at a high level, approved your project to begin using cloud services. However, the committee is concerned with getting locked into a single cloud provider and has flagged the ability to easily move between cloud providers as a top priority. It also wants to save costs by reusing components.
Which cross-cutting aspect of cloud computing would be your primary focus as your project plan continues to develop and you begin to evaluate cloud providers?

A. Interoperability
B. Resiliency
C. Scalability
D. Portability

Answer: A

Explanation:
Interoperability is ability to easily move between cloud providers, by either moving or reusing components and services. This can pertain to any cloud deployment model, and it gives organizations the ability to constantly evaluate costs and services as well as move their business to another cloud provider as needed or desired. Portability relates to the wholesale moving of services from one cloud provider to another, not necessarily the reuse of components or services for other purposes. Although resiliency is not an official concept within cloud computing, it certainly would be found throughout other topics such as elasticity, auto-scaling, and resource pooling. Scalability pertains to changing resource allocations to a service to meet current demand, either upward or downward in scope.

NEW QUESTION 151
- (Exam Topic 4)
Which of the following is the primary purpose of an SOC 3 report?

A. HIPAA compliance
B. Absolute assurances
C. Seal of approval
D. Compliance with PCI/DSS

Answer: C

Explanation:
The SOC 3 report is more of an attestation than a full evaluation of controls associated with a service provider.

NEW QUESTION 155
- (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 160
- (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 164
- (Exam Topic 4)
Which of the following is NOT one of the official risk rating categories?

A. Critical
B. Low

C. Catastrophic
D. Minimal

Answer: C

Explanation:
The official categories of cloud risk ratings are Minimal, Low, Moderate, High, and Critical.

NEW QUESTION 167
- (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 169
- (Exam Topic 3)
You are working for a cloud service provider and receive an eDiscovery order pertaining to one of your customers.
Which of the following would be the most appropriate action to take first?

A. Take a shapshot of the virtual machines
B. Escrow the encryption keys
C. Copy the data
D. Notify the customer

Answer: D

Explanation:
When a cloud service provider receives an eDiscovery order pertaining to one of their customers, the first action they must take is to notify the customer. This allows the customer to be aware of what was received, as well as to conduct a review to determine if any challenges are necessary or warranted. Taking snapshots of virtual machines, copying data, and escrowing encryption keys are all processes involved in the actual collection of data and should not be performed until the customer has been notified of the request.

NEW QUESTION 174
- (Exam Topic 3)
What is a serious complication an organization faces from the compliance perspective with international operations?

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

Answer: A

Explanation:
When operating within a global framework, a security professional runs into a multitude of jurisdictions and requirements, which often may not be clearly applicable or may be in contention with each other. These requirements can involve 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, and finally the appropriate laws and regulations for the jurisdiction housing the IT resources and where the data is actually stored, which may be multiple jurisdictions as well. Different certifications would not come into play as a challenge because the major IT and data center certifications are international and would apply to any cloud provider. Different capabilities and different operational procedures would be mitigated by the organization's selection of a cloud provider and would not be a challenge if an appropriate provider was chosen, regardless of location.

NEW QUESTION 179
- (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 181
- (Exam Topic 3)
The European Union is often considered the world leader in regard to the privacy of personal data and has declared privacy to be a "human right."
In what year did the EU first assert this principle?

A. 1995
B. 2000
C. 2010
D. 1999

Answer: A

Explanation:
SThe EU passed Directive 95/46 EC in 1995, which established data privacy as a human right. The other years listed are incorrect.

NEW QUESTION 184
- (Exam Topic 3)
Which of the following systems is used to employ a variety of different techniques to discover and alert on threats and potential threats to systems and networks?

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

Answer: A

Explanation:
An intrusion detection system (IDS) is implemented to watch network traffic and operations, using predefined criteria or signatures, and alert administrators if anything suspect is found. An intrusion prevention system (IPS) is similar to an IDS but actually takes action against suspect traffic, whereas an IDS just alerts when it finds anything suspect. A firewall works at the network level and only takes into account IP addresses, ports, and protocols; it does not inspect the traffic for patterns or content. A web application firewall (WAF) works at the application layer and provides additional security via proxying, filtering service requests, or blocking based on additional factors such as the client and requests.

NEW QUESTION 188
- (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 192
- (Exam Topic 3)
What does a cloud customer purchase or obtain from a cloud provider?

A. Services
B. Hosting
C. Servers
D. Customers

Answer: A

Explanation:
No matter what form they come in, "services" are obtained or purchased by a cloud customer from a cloud service provider. Services can come in many forms--virtual machines, network configurations, hosting setups, and software access, just to name a few. Hosting and servers--or, with a cloud, more appropriately virtual machines--are just two examples of "services" that a customer would purchase from a cloud provider. "Customers" would never be a service that's purchased.

NEW QUESTION 196
- (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 201
- (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 206
- (Exam Topic 3)
With software-defined networking (SDN), which two types of network operations are segregated to allow for granularity and delegation of administrative access and functions?

A. Filtering and forwarding
B. Filtering and firewalling
C. Firewalling and forwarding
D. Forwarding and protocol

Answer: A

Explanation:
With SDN, the filtering and forwarding capabilities and administration are separated. This allows the cloud provider to build interfaces and management tools for administrative delegation of filtering configuration, without having to allow direct access to underlying network equipment. Firewalling and protocols are both terms related to networks, but they are not components SDN is concerned with.

NEW QUESTION 207
- (Exam Topic 3)
DNSSEC was designed to add a layer of security to the DNS protocol. Which type of attack was the DNSSEC extension designed to mitigate?

A. Account hijacking
B. Snooping
C. Spoofing
D. Data exposure

Answer: C

Explanation:
DNSSEC is an extension to the regular DNS protocol that utilizes digital signing of DNS query results, which can be verified to come from an authoritative source. This verification mitigates the ability for a rogue DNS server to be used to spoof query results and to direct users to malicious sites. DNSSEC provides for the verification of the integrity of DNS queries. It does not provide any protection from snooping or data exposure. Although it may help lessen account hijacking by preventing users from being directed to rogue sites, it cannot by itself eliminate the possibility.

NEW QUESTION 212
- (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 215
- (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 217
- (Exam Topic 3)
Which of the following roles would be responsible for managing memberships in federations and the use and integration of federated services?

A. Inter-cloud provider
B. Cloud service business manager
C. Cloud service administrator
D. Cloud service integrator

Answer: A

Explanation:
The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated 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 integrator is responsible for connecting existing systems and services with a cloud. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

NEW QUESTION 222
- (Exam Topic 3)
Which of the following statements best describes a Type 1 hypervisor?

A. The hypervisor software runs within an operating system tied to the hardware.
B. The hypervisor software runs as a client on a server and needs an external service to administer it.
C. The hypervisor software runs on top of an application layer.
D. The hypervisor software runs directly on “bare metal” without an intermediary.

Answer: D

Explanation:
With a Type 1 hypervisor, the hypervisor software runs directly on top of the bare-metal system, without any intermediary layer or hosting system. None of these statements describes a Type 1 hypervisor.

NEW QUESTION 227
- (Exam Topic 3)
In the wake of many scandals with major corporations involving fraud and the deception of investors and regulators, which of the following laws was passed to govern accounting and financial records and disclosures?

A. GLBA
B. Safe Harbor
C. HIPAA
D. SOX

Answer: D

Explanation:
The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and accounting errors.The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy. The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Safe Harbor program was designed by the US government as a way for American companies to comply with European Union privacy laws.

NEW QUESTION 229
- (Exam Topic 3)
Most APIs will support a variety of different data formats or structures.
However, the SOAP API will only support which one of the following data formats?

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

Answer: A

Explanation:
The Simple Object Access Protocol (SOAP) protocol only supports the Extensible Markup Language (XML) data format. Although the other options are all data formats or data structures, they are not supported by SOAP.

NEW QUESTION 234
- (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 238
- (Exam Topic 3)
Along with humidity, temperature is crucial to a data center for optimal operations and protection of equipment.
Which of the following is the optimal temperature range as set by ASHRAE?

A. 69.8 to 86.0 degrees Fahrenheit (21 to 30 degrees Celsius)
B. 51.8 to 66.2 degrees Fahrenheit (11 to 19 degrees Celsius)
C. 64.4 to 80.6 degrees Fahrenheit (18 to 27 degrees Celsius)
D. 44.6 to 60.8 degrees Fahrenheit (7 to 16 degrees Celsius)

Answer: C

Explanation:
The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) recommends

NEW QUESTION 239
- (Exam Topic 3)
Which of the following threat types involves leveraging a user's browser to send untrusted data to be executed with legitimate access via the user's valid credentials?

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

Answer: D

Explanation:
Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or perhaps the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with their own access and permissions, allowing the attacker to redirect the user's web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access. 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 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 242
- (Exam Topic 3)
With IaaS, what is responsible for handling the security and control over the volume storage space?

A. Management plane
B. Operating system
C. Application
D. Hypervisor

Answer: B

Explanation:
Volume storage is allocated via a LUN to a system and then treated the same as any traditional storage. The operating system is responsible for formatting and securing volume storage as well as controlling all access to it. Applications, although they may use volume storage and have permissions to write to it, are not responsible for its formatting and security. Both a hypervisor and the management plane are outside of an individual system and are not responsible for managing the files and storage within that system.

NEW QUESTION 243
- (Exam Topic 3)

What type of storage structure does object storage employ to maintain files?

A. Directory
B. Hierarchical
C. tree
D. Flat

Answer: D

Explanation:
Object storage uses a flat file system to hold storage objects; it assigns files a key value that is then used to access them, rather than relying on directories or descriptive filenames. Typical storage layouts such as tree, directory, and hierarchical structures are used within volume storage, whereas object storage maintains a flat structure with key values.

NEW QUESTION 248
- (Exam Topic 3)
Where is a DLP solution generally installed when utilized for monitoring data in use?

A. Application server
B. Database server
C. Network perimeter
D. User's client

Answer: D

Explanation:
To monitor data in use, the DLP solution's optimal location would be on the user's client or workstation, where the data would be used or processed, and where it would be most vulnerable to access or exposure. The network perimeter is most appropriate for data in transit, and an application server would serve as middle stage between data at rest and data in use, but is a less correct answer than a user's client. A database server would be an example of a location appropriate for monitoring data at rest.

NEW QUESTION 250
- (Exam Topic 3)
In order to comply with regulatory requirements, which of the following secure erasure methods would be available to a cloud customer using volume storage within the IaaS service model?

A. Demagnetizing
B. Shredding
C. Degaussing
D. Cryptographic erasure

Answer: D

Explanation:
Cryptographic erasure is a secure method to destroy data by destroying the keys that were used to encrypt it. This method is universally available for volume storage on IaaS and is also extremely quick. Shredding, degaussing, and demagnetizing are all physically destructive methods that would not be permitted within a cloud environment using shared resources.

NEW QUESTION 255
- (Exam Topic 3)
Many different common threats exist against web-exposed services and applications. One attack involves attempting to leverage input fields to execute queries in a nested fashion that is unintended by the developers.
What type of attack is this?

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

Answer: A

Explanation:
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. This can trick an application into exposing data that is not intended or authorized to be exposed, or it can potentially allow an attacker to gain insight into configurations or security controls. 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. 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. 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 258
- (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 260
- (Exam Topic 3)
When dealing with PII, which category pertains to those requirements that can carry legal sanctions or penalties for failure to adequately safeguard the data and address compliance requirements?

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

Answer: C

Explanation:
Regulated PII pertains to data that is outlined in law and regulations. Violations of the requirements for the protection of regulated PII can carry legal sanctions or penalties. Contractual PII involves required data protection that is determined by the actual service contract between the cloud provider and cloud customer, rather than outlined by law. Violations of the provisions of contractual PII carry potential financial or contractual implications, but not legal sanctions. Legal and jurisdictional are similar terms to regulated, but neither is the official term used.

NEW QUESTION 263
- (Exam Topic 3)
Within a SaaS environment, what is the responsibility on the part of the cloud customer in regard to procuring the software used?

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

Answer: B

Explanation:
Within a SaaS implementation, the cloud customer licenses the use of the software from the cloud provider
because SaaS delivers a fully functional application to the customer. With SaaS, the cloud provider is responsible for the entire software application and any necessary infrastructure to develop, run, and maintain it. The purchasing, development, and maintenance are fully the responsibility of the cloud provider.

NEW QUESTION 267
- (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 269
- (Exam Topic 3)
Different types of audits are intended for different audiences, such as internal, external, regulatory, and so on. Which of the following audits are considered "restricted use" versus being for a more broad audience?

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

Answer: B

Explanation:
SOC Type 1 reports are intended for restricted use, only to be seen by the actual service organization, its current clients, or its auditors. These reports are not intended for wider or public distribution.SAS-70 audit reports have been deprecated and are no longer in use, and both the SOC Type 2 and 3 reports are designed to expand upon the SOC Type 1 reports and are for broader audiences.

NEW QUESTION 272
- (Exam Topic 3)
Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.
Which of the following is NOT a regulatory system from the United States federal government?

A. HIPAA
B. SOX
C. FISMA
D. PCI DSS

Answer: D

Explanation:
The Payment Card Industry Data Security Standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry-regulatory standard, not a governmental one. The Sarbanes-Oxley Act (SOX) was passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders. The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

NEW QUESTION 276
- (Exam Topic 3)
You just hired an outside developer to modernize some applications with new web services and functionality. In order to implement a comprehensive test platform for validation, the developer needs a data set that resembles a production data set in both size and composition.
In order to accomplish this, what type of masking would you use?

A. Development
B. Replicated
C. Static
D. Dynamic

Answer: C

Explanation:
Static masking takes a data set and produces a copy of it, but with sensitive data fields masked. This allows for a full data set from production for testing purposes, but without any sensitive data. Dynamic masking works with a live system and is not used to produce a distinct copy. The terms "replicated" and "development" are not types of masking.

NEW QUESTION 278
- (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 283
- (Exam Topic 3)
Implementing baselines on systems would take an enormous amount of time and resources if the staff had to apply them to each server, and over time, it would be almost impossible to keep all the systems in sync on an ongoing basis.
Which of the following is NOT a package that can be used for implementing and maintaining baselines across an enterprise?

A. Puppet
B. SCCM
C. Chef
D. GitHub

Answer: D

Explanation:
GitHub is a software development platform that serves as a code repository and versioning system. It is solely used for software development and would not be appropriate for applying baselines to systems. Puppet is an open-source configuration management tool that runs on many platforms and can be used to apply and maintain baselines. The Software Center Configuration Manager (SCCM) was developed by Microsoft for managing systems across large groups of servers. Chef is also a system for maintaining large groups of systems throughout an enterprise.

NEW QUESTION 286
- (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 290
- (Exam Topic 3)
Which phase of the cloud data lifecycle would be the MOST appropriate for the use of DLP technologies to protect the data?

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

Answer: C

Explanation:
During the share phase, data is allowed to leave the application for consumption by other vendors, systems, or services. At this point, as the data is leaving the security controls of the application, the use of DLP technologies is appropriate to control how the data is used or to force expiration. During the use, create, and store phases, traditional security controls are available and are more appropriate because the data is still internal to the application.

NEW QUESTION 291
- (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 293
- (Exam Topic 2)
Which OSI layer does IPsec operate at?

A. Network
B. transport
C. Application
D. Presentation

Answer: A

Explanation:
A major difference between IPsec and other protocols such as TLS is that IPsec operates at the Internet network layer rather than the application layer, allowing for complete end-to-end encryption of all communications and traffic.

NEW QUESTION 294
- (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 296
- (Exam Topic 2)
What does the "SOC" acronym refer to with audit reports?

A. Service Origin Confidentiality
B. System Organization Confidentiality
C. Service Organizational Control
D. System Organization Control

Answer: C

NEW QUESTION 300
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the requirements placed on a system or application by law, policy, or requirements from standards?

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

Answer: A

Explanation:
Regulatory requirements are those imposed upon businesses and their operations either by law, regulation, policy, or standards and guidelines. These requirements are specific either to the locality in which the company or application is based or to the specific nature of the data and transactions conducted.

NEW QUESTION 304
- (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 305
- (Exam Topic 2)
Which of the following does NOT fall under the "IT" aspect of quality of service (QoS)?

A. Applications
B. Key performance indicators (KPIs)
C. Services
D. Security

Answer: B

Explanation:
KPIs fall under the "business" aspect of QoS, along with monitoring and measuring of events and business processes. Services, security, and applications are all core components and concepts of the "IT" aspect of QoS.

NEW QUESTION 310
- (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 312
- (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 317
- (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 323
- (Exam Topic 2)
What concept does the "D" represent with the STRIDE threat model?

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

Answer: B

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 non-authenticated 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.

NEW QUESTION 325
- (Exam Topic 2)
Which of the following is NOT a function performed by the record protocol of TLS?

A. Encryption
B. Acceleration
C. Authentication
D. Compression

Answer: B

Explanation:
The record protocol of TLS performs the authentication and encryption of data packets, and in some cases compression as well. It does not perform any acceleration functions.

NEW QUESTION 329
- (Exam Topic 2)
From a security perspective, which of the following is a major concern when evaluating possible BCDR solutions?

A. Access provisioning
B. Auditing
C. Jurisdictions
D. Authorization

Answer: C

Explanation:

When a security professional is considering cloud solutions for BCDR, a top concern is the jurisdiction where the cloud systems are hosted. If the jurisdiction is different from where the production systems are hosted, they may be subjected to different regulations and controls, which would make a seamless BCDR solution far more difficult.

NEW QUESTION 333
- (Exam Topic 2)
Which audit type has been largely replaced by newer approaches since 2011?

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

Answer: C

Explanation:
SAS-70 reports were replaced in 2011 with the SSAE-16 reports throughout the industry.

NEW QUESTION 335
- (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 336
- (Exam Topic 2)
Which of the following service categories entails the least amount of support needed on the part of the cloud customer?

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

Answer: A

Explanation:
With SaaS providing a fully functioning application that is managed and maintained by the cloud provider, cloud customers incur the least amount of support responsibilities themselves of any service category.

NEW QUESTION 339
- (Exam Topic 2)
Which value refers to the percentage of production level restoration needed to meet BCDR objectives?

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

Answer: C

Explanation:
The recovery service level (RSL) is a percentage measure of the total typical production service level that needs to be restored to meet BCDR objectives in the case of a failure.

NEW QUESTION 341
- (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 346
- (Exam Topic 2)
Which security concept is based on preventing unauthorized access to data while also ensuring that it is accessible to those authorized to use it?

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

Answer: C

Explanation:
The main goal of confidentiality is to ensure that sensitive information is not made available or leaked to parties that should not have access to it, while at the same time ensuring that those with appropriate need and authorization to access it can do so in a manner commensurate with their needs and confidentiality requirements.

NEW QUESTION 351
- (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 353
- (Exam Topic 2)
Which regulatory system pertains to the protection of healthcare data?

A. HIPAA
B. HAS
C. HITECH
D. HFCA

Answer: A

Explanation:
The Health Insurance Portability and Accountability Act (HIPAA) sets stringent requirements in the United States for the protection of healthcare records.

NEW QUESTION 358
- (Exam Topic 2)
What type of security threat is DNSSEC designed to prevent?

A. Account hijacking
B. Snooping
C. Spoofing
D. Injection

Answer: C

Explanation:
DNSSEC is designed to prevent the spoofing and redirection of DNS resolutions to rogue sites.

NEW QUESTION 360
- (Exam Topic 2)
What process is used within a clustered system to provide high availability and load balancing?

A. Dynamic balancing
B. Dynamic clustering
C. Dynamic optimization
D. Dynamic resource scheduling

Answer: D

Explanation:
Dynamic resource scheduling (DRS) is used within all clustering systems as the method for clusters to provide high availability, scaling, management, and workload distribution and balancing of jobs and processes. From a physical infrastructure perspective, DRS is used to balance compute loads between physical hosts in a cloud to maintain the desired thresholds and limits on the physical hosts.

NEW QUESTION 363
- (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 366
- (Exam Topic 2)
Which attribute of data poses the biggest challenge for data discovery?

A. Labels
B. Quality
C. Volume
D. Format

Answer: B

Explanation:
The main problem when it comes to data discovery is the quality of the data that analysis is being performed against. Data that is malformed, incorrectly stored or labeled, or incomplete makes it very difficult to use analytical tools against.

NEW QUESTION 370
- (Exam Topic 2)
Which of the following technologies is used to monitor network traffic and notify if any potential threats or attacks are noticed?

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

Answer: D

Explanation:
An intrusion detection system (IDS) is designed to analyze network packets, compare their contents or characteristics against a set of configurations or signatures, and alert personnel if anything is detected that could constitute a threat or is otherwise designated for alerting.

NEW QUESTION 372
- (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 377
- (Exam Topic 2)
Which of the following is NOT one of five principles of SOC Type 2 audits?

A. Privacy
B. Processing integrity
C. Financial
D. Security

Answer: C

Explanation:
The SOC Type 2 audits include five principles: security, privacy, processing integrity, availability, and confidentiality.

NEW QUESTION 380

- (Exam Topic 2)
What strategy involves hiding data in a data set to prevent someone from identifying specific individuals based on other data fields present?

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

Answer: A

Explanation:
With data anonymization, data is manipulated in such a way so as to prevent the identification of an individual through various data objects, and is often used in conjunction with other concepts such as masking.

NEW QUESTION 381
- (Exam Topic 2)
Which data point that auditors always desire is very difficult to provide within a cloud environment?

A. Access policy
B. Systems architecture
C. Baselines
D. Privacy statement

Answer: B

Explanation:
Cloud environments are constantly changing and often span multiple physical locations. A cloud customer is also very unlikely to have knowledge and insight into the underlying systems architecture in a cloud environment. Both of these realities make it very difficult, if not impossible, for an organization to provide a comprehensive systems design document.

NEW QUESTION 383
- (Exam Topic 2)
What does the REST API use to protect data transmissions?

A. NetBIOS
B. VPN
C. Encapsulation
D. TLS

Answer: D

Explanation:
Representational State Transfer (REST) uses TLS for communication over secured channels. Although REST also supports SSL, at this point SSL has been phased out due to vulnerabilities and has been replaced by TLS.

NEW QUESTION 386
- (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 388
- (Exam Topic 2)
Which of the following is a restriction that can be enforced by information rights management (IRM) that is not possible for traditional file system controls?

A. Delete
B. Modify
C. Read
D. Print

Answer: D

Explanation:
IRM allows an organization to control who can print a set of information. This is not be possible under traditional file system controls, where if a user can read a file, they are able to print it as well.

NEW QUESTION 389
- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the ability for a cloud customer to easily remove their applications and data from a cloud environment?

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

Answer: A

Explanation:
Reversibility is the ability for a cloud customer to easily remove their applications or data from a cloud environment, as well as to ensure that all traces of their applications or data have been securely removed per a predefined agreement with the cloud provider.

NEW QUESTION 390
- (Exam Topic 2)
What is the minimum regularity for testing a BCDR plan to meet best practices?

A. Once year
B. Once a month
C. Every six months
D. When the budget allows it

Answer: A

Explanation:
Best practices and industry standards dictate that a BCDR solution should be tested at least once a year, though specific regulatory requirements may dictate more regular testing. The BCDR plan should also be tested whenever a major modification to a system occurs.

NEW QUESTION 391
- (Exam Topic 1)
Which of the following publishes the most commonly used standard for data center design in regard to tiers and topologies?

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

Answer: B

Explanation:
The Uptime Institute publishes the most commonly used and widely known standard on data center tiers and topologies. It is based on a series of four tiers, with each progressive increase in number representing more stringent, reliable, and redundant systems for security, connectivity, fault tolerance, redundancy, and cooling.

NEW QUESTION 395
- (Exam Topic 1)
Which of the following roles is responsible for peering with other cloud services and providers?

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

Answer: B

Explanation:
The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated services.

NEW QUESTION 400
- (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 402
- (Exam Topic 1)
Which of the following is NOT a criterion for data within the scope of eDiscovery?

A. Possession
B. Custody
C. Control
D. Archive

Answer: D

Explanation:
eDiscovery pertains to information and data that is in the possession, control, and custody of an organization.

NEW QUESTION 406
- (Exam Topic 1)
From a legal perspective, what is the most important first step after an eDiscovery order has been received by the cloud provider?

A. Notification
B. Key identification
C. Data collection
D. Virtual image snapshots

Answer: A

Explanation:
The contract should include requirements for notification by the cloud provider to the cloud customer upon the receipt of such an order. This serves a few important purposes. First, it keeps communication and trust open between the cloud provider and cloud customers. Second, and more importantly, it allows the cloud customer to potentially challenge the order if they feel they have the grounds or desire to do so.

NEW QUESTION 409
- (Exam Topic 1)
Which aspect of archiving must be tested regularly for the duration of retention requirements?

A. Availability
B. Recoverability
C. Auditability
D. Portability

Answer: B

Explanation:
In order for any archiving system to be deemed useful and compliant, regular tests must be performed to ensure the data can still be recovered and accessible, should it ever be needed, for the duration of the retention requirements.

NEW QUESTION 413
- (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 414
- (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 416
- (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 420
- (Exam Topic 1)
What is the biggest benefit to leasing space in a data center versus building or maintain your own?

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

Answer: B

Explanation:
When leasing space in a data center, an organization can avoid the enormous startup and building costs associated with a data center, and can instead leverage economies of scale by grouping with other organizations and sharing costs.

NEW QUESTION 422
- (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 427
- (Exam Topic 1)
Which of the following pertains to a macro level approach to data center design rather than the traditional tiered approach to data centers?

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

Answer: A

Explanation:
The standards put out by the International Data Center Authority (IDCA) have established the Infinity Paradigm, which is intended to be a comprehensive data center design and operations framework. The Infinity Paradigm shifts away from many models that rely on tiered architecture for data centers, where each successive tier increases redundancy. Instead, it emphasizes data centers being approached at a macro level, without a specific and isolated focus on certain aspects to achieve tier status.

NEW QUESTION 432
- (Exam Topic 1)
Which of the following cloud aspects complicates eDiscovery?

A. Resource pooling
B. On-demand self-service
C. Multitenancy
D. Measured service

Answer: C

Explanation:
With multitenancy, eDiscovery becomes more complicated because the data collection involves extra steps to ensure that only those customers or systems that are within scope are turned over to the requesting authority.

NEW QUESTION 433
- (Exam Topic 1)
Which term relates to the application of scientific methods and practices to evidence?

A. Forensics
B. Methodical
C. Theoretical
D. Measured

Answer: A

Explanation:
Forensics is the application of scientific and methodical processes to identify, collect, preserve, analyze, and summarize/report digital information and evidence.

NEW QUESTION 435
- (Exam Topic 1)
What type of PII is regulated based on the type of application or per the conditions of the specific hosting agreement?

A. Specific
B. Contractual
C. regulated
D. Jurisdictional

Answer: B

Explanation:
Contractual PII has specific requirements for the handling of sensitive and personal information, as defined at a contractual level. These specific requirements will typically document the required handling procedures and policies to deal with PII. They may be in specific security controls and configurations, required policies or procedures, or limitations on who may gain authorized access to data and systems.

NEW QUESTION 436
- (Exam Topic 1)
Which of the following represents a control on the maximum amount of resources that a single customer, virtual machine, or application can consume within a cloud environment?

A. Share
B. Reservation
C. Provision
D. Limit

Answer: D

Explanation:
Limits are put in place to enforce a maximum on the amount of memory or processing a cloud customer can use. This can be done either on a virtual machine or as a comprehensive whole for a customer, and is meant to ensure that enormous cloud resources cannot be allocated or consumed by a single host or customer to the detriment of other hosts and customers.

NEW QUESTION 439
- (Exam Topic 1)
Which of the following roles involves the connection and integration of existing systems and services to a cloud environment?

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

Answer: D

Explanation:
The cloud service integrator is the official role that involves connecting and integrating existing systems and services with a cloud environment. This may involve moving services into a cloud environment, or connecting to external cloud services and capabilities from traditional data center-hosted services.

NEW QUESTION 442
- (Exam Topic 1)
Which of the following represents a prioritization of applications or cloud customers for the allocation of additional requested resources when there is a limitation on available resources?

A. Provision
B. Limit
C. Reservation
D. Share

Answer: D

Explanation:
The concept of shares within a cloud environment is used to mitigate and control the request for resource allocations from customers that the environment may not have the current capability to allow. Shares work by prioritizing hosts within a cloud environment through a weighting system that is defined by the cloud provider. When periods of high utilization and allocation are reached, the system automatically uses scoring of each host based on its share value to determine which hosts get access to the limited resources still available. The higher the value a particular host has, the more resources it will be allowed to utilize.

NEW QUESTION 445
- (Exam Topic 1)
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 449
- (Exam Topic 1)
What type of masking strategy involves making a separate and distinct copy of data with masking in place?

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

Answer: C

Explanation:
With static masking, a separate and distinct copy of the data set is created with masking in place. This is typically done through a script or other process that takes a standard data set, processes it to mask the appropriate and predefined fields, and then outputs the data set as a new one with the completed masking done.

NEW QUESTION 450
- (Exam Topic 1)
Which of the following roles is responsible for obtaining new customers and securing contracts and agreements?

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

Answer: B

Explanation:
The cloud service broker is responsible for obtaining new customers, analyzing the marketplace, and securing contracts and agreements.

NEW QUESTION 454
- (Exam Topic 1)
Which of the following is considered an internal redundancy for a data center?

A. Power distribution units
B. Network circuits
C. Power substations
D. Generators

Answer: A

Explanation:
Power distribution units are internal to a data center and supply power to internal components such as racks, appliances, and cooling systems. As such, they are considered an internal redundancy.

NEW QUESTION 456
- (Exam Topic 1)
Which of the following APIs are most commonly used within a cloud environment?

A. REST and SAML
B. SOAP and REST
C. REST and XML
D. XML and SAML

Answer: B

Explanation:
Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) are the most commonly used APIs within a cloud environment. 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.

NEW QUESTION 457
- (Exam Topic 1)
Which of the following security measures done at the network layer in a traditional data center are also applicable to a cloud environment?

A. Dedicated switches
B. Trust zones
C. Redundant network circuits
D. Direct connections

Answer: B

Explanation:
Trust zones can be implemented to separate systems or tiers along logical lines for great security and access controls. Each zone can then have its own security controls and monitoring based on its particular needs.

NEW QUESTION 459
- (Exam Topic 1)
What does the REST API support that SOAP does NOT support?

A. Caching
B. Encryption
C. Acceleration
D. Redundancy

Answer: A

Explanation:
The SOAP protocol does not support caching, whereas the REST API does.

NEW QUESTION 462
- (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 465
- (Exam Topic 1)
Which of the following is the biggest concern or challenge with using encryption?

A. Dependence on keys
B. Cipher strength
C. Efficiency
D. Protocol standards

Answer: A

Explanation:
No matter what kind of application, system, or hosting model used, encryption is 100 percent dependent on
encryption keys. Properly securing the keys and the exchange of them is the biggest and most important challenge of encryption systems.

NEW QUESTION 467
- (Exam Topic 1)
Which of the following threat types involves an application developer leaving references to internal information and configurations in code that is exposed to the client?

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

Answer: C

Explanation:
An insecure direct object reference occurs when a developer has in their code a reference to something on the application side, such as a database key, the directory structure of the application, configuration information about the hosting system, or any other information that pertains to the workings of the application that should not be exposed to users or the network. Unvalidated redirects and forwards occur when an application has functions to forward users to other sites, and these functions are not properly secured to validate the data and redirect requests, allowing spoofing for malware of phishing attacks. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data. Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner.

NEW QUESTION 469
- (Exam Topic 1)
Which of the following threat types involves the sending of untrusted data to a user's browser to be executed with their own credentials and access?

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

D. Injection

Answer: B

Explanation:
Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or where the code is not properly
escaped from processing by the browser. The code is then executed on the user's browser with the user's own access and permissions, allowing an attacker to redirect their web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access.

NEW QUESTION 471
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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