ISC2

Exam Questions CCSP

Certified Cloud Security Professional

NEW QUESTION 1
- (Exam Topic 4)
Countermeasures for protecting cloud operations against external attackers include all of the following except:

A. Continual monitoring for anomalous activity.
B. Detailed and extensive background checks.
C. Regular and detailed configuration/change management activities
D. Hardened devices and systems, including servers, hosts, hypervisors, and virtual machines.

Answer: B

Explanation:
Background checks are controls for attenuating potential threats from internal actors; external threats aren't likely to submit to background checks.

NEW QUESTION 2
- (Exam Topic 4)
Which of the following storage types is most closely associated with a database-type storage implementation?

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

Answer: D

Explanation:
Structured storage involves organized and categorized data, which most closely resembles and operates like a database system would.

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

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

Answer: A

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

NEW QUESTION 4
- (Exam Topic 4)
Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?

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

Answer: B

Explanation:
SOC 2 deals with the CIA triad. SOC 1 is for financial reporting. SOC 3 is only an attestation by the auditor. There is no SOC 4.

NEW QUESTION 5
- (Exam Topic 4)
With the rapid emergence of cloud computing, very few regulations were in place that pertained to it specifically, and organizations often had to resort to using a collection of regulations that were not specific to cloud in order to drive audits and policies.
Which standard from the ISO/IEC was designed specifically for cloud computing?

A. ISO/IEC 27001
B. ISO/IEC 19889
C. ISO/IEC 27001:2015
D. ISO/IEC 27018

Answer: D

Explanation:

ISO/IEC 27018 was implemented to address the protection of personal and sensitive information within a cloud environment. ISO/IEC 27001 and its later 27001:2015 revision are both general-purpose data security standards. ISO/IEC 19889 is an erroneous answer.

NEW QUESTION 6
- (Exam Topic 4)
Tokenization requires two distinct _____.

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

Answer: D

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

NEW QUESTION 7
- (Exam Topic 4)
A variety of security systems can be integrated within a network--some that just monitor for threats and issue alerts, and others that take action based on signatures, behavior, and other types of rules to actively stop potential threats.
Which of the following types of technologies is best described here?

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

Answer: B

Explanation:
An intrusion prevention system (IPS) can inspect traffic and detect any suspicious traffic based on a variety of factors, but it can also actively block such traffic. Although an IDS can detect the same types of suspicious traffic as an IPS, it is only design to alert, not to block. A firewall is only concerned with IP addresses, ports, and protocols; it cannot be used for the signature-based detection of traffic. A proxy can limit or direct traffic based on more extensive factors than a network firewall can, but it's not capable of using the same signature detection rules as an IPS.

NEW QUESTION 8
- (Exam Topic 4)
What is the experimental technology that might lead to the possibility of processing encrypted data without having to decrypt it first?

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

Answer: C

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

NEW QUESTION 9
- (Exam Topic 4)
Which of the following jurisdictions lacks a comprehensive national policy on data privacy and the protection of personally identifiable information (PII)?

A. European Union
B. Asian-Pacific Economic Cooperation
C. United States
D. Russia

Answer: C

Explanation:
The United States has a myriad of regulations focused on specific types of data, such as healthcare and financial, but lacks an overall comprehensive privacy law on the national level. The European Union, the Asian-Pacific Economic Cooperation, and Russia all have national privacy protections and regulations for the handling the PII data of their citizens.

NEW QUESTION 10
- (Exam Topic 4)
The cloud customer's trust in the cloud provider can be enhanced by all of the following except:

A. SLAs
B. Shared administration
C. Audits
D. real-time video surveillance

Answer:

D

Explanation:
Video surveillance will not provide meaningful information and will not enhance trust. All the others will do it.

NEW QUESTION 10
- (Exam Topic 4)
What is one of the reasons a baseline might be changed?

A. Numerous change requests
B. To reduce redundancy
C. Natural disaster
D. Power fluctuation

Answer: A

Explanation:
If the CMB is receiving numerous change requests to the point where the amount of requests would drop by modifying the baseline, then that is a good reason to change the baseline. None of the other reasons should involve the baseline at all.

NEW QUESTION 14
- (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 16
- (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 21
- (Exam Topic 4)
Because of multitenancy, specific risks in the public cloud that don't exist in the other cloud service models include all the following except:

A. DoS/DDoS
B. Information bleed
C. Risk of loss/disclosure due to legal seizures
D. Escalation of privilege

Answer: A

Explanation:
DoS/DDoS threats and risks are not unique to the public cloud model.

NEW QUESTION 24
- (Exam Topic 4)
Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider?

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

Answer: C

Explanation:
The SOC 3 is the least detailed, so the provider is not concerned about revealing it. The SOC 1 Types 1 and 2 are about financial reporting, and not relevant. The

SOC 2 Type 2 is much more detailed and will most likely be kept closely held by the provider.

NEW QUESTION 29
- (Exam Topic 4)
Which format is the most commonly used standard for exchanging information within a federated identity system?

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

Answer: C

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

NEW QUESTION 31
- (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 36
- (Exam Topic 4)
In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?

A. Physical
B. All of the above
C. technological
D. Administrative

Answer: B

Explanation:
Layered defense calls for a diverse approach to security.

NEW QUESTION 37
- (Exam Topic 4)
Which of the following is NOT considered a type of data loss?

A. Data corruption
B. Stolen by hackers
C. Accidental deletion
D. Lost or destroyed encryption keys

Answer: B

Explanation:
The exposure of data by hackers is considered a data breach. Data loss focuses on the data availability rather than security. Data loss occurs when data becomes lost, unavailable, or destroyed, when it should not have been.

NEW QUESTION 42
- (Exam Topic 4)
Above and beyond general regulations for data privacy and protection, certain types of data are subjected to more rigorous regulations and oversight.
Which of the following is not a regulatory framework for more sensitive or specialized data?

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

Answer: A

Explanation:
The FIPS 140-2 standard pertains to the certification of cryptographic modules and is not a regulatory framework. The Payment Card Industry Data Security Standard (PCI DSS), the Federal Risk and
Authorization Management Program (FedRAMP), and the Health Insurance Portability and Accountability Act (HIPAA) are all regulatory frameworks for sensitive or specialized data.

NEW QUESTION 45
- (Exam Topic 4)
Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:

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

Answer: C

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

NEW QUESTION 47
- (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 50
- (Exam Topic 4)
What are third-party providers of IAM functions for the cloud environment?

A. AESs
B. SIEMs
C. DLPs
D. CASBs

Answer: D

Explanation:
Data loss, leak prevention, and protection is a family of tools used to reduce the possibility of unauthorized disclosure of sensitive information. SIEMs are tools used to collate and manage log data. AES is an encryption standard.

NEW QUESTION 52
- (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 53
- (Exam Topic 4)
Which of the following are considered to be the building blocks of cloud computing?

A. CPU, RAM, storage, and networking
B. Data, CPU, RAM, and access control
C. Data, access control, virtualization, and services
D. Storage, networking, printing, and virtualization

Answer: A

NEW QUESTION 55
- (Exam Topic 4)
Data masking can be used to provide all of the following functionality, except:

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

Answer: C

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

NEW QUESTION 57
- (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 60
- (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 65
- (Exam Topic 4)
When using an IaaS solution, what is a key benefit provided to the customer?

A. Metered and priced on the basis of units consumed
B. Increased energy and cooling system efficiencies
C. Transferred cost of ownership
D. The ability to scale up infrastructure services based on projected usage

Answer: A

Explanation:
IaaS has a number of key benefits for organizations, which include but are not limited to these: -- - Usage is metered and priced on the basis of units (or instances) consumed. This can also be billed back to specific departments or functions.
- It has an ability to scale up and down infrastructure services based on actual usage. This is particularly useful and beneficial where there are significant spikes and dips within the usage curve for infrastructure.
- It has a reduced cost of ownership. There is no need to buy assets for everyday use, no loss of asset value over time, and reduced costs of maintenance and support.
- It has a reduced energy and cooling costs along with "green IT" environment effect with optimum use of IT resources and systems.

NEW QUESTION 70
- (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 75
- (Exam Topic 4)
Which of the following is NOT a commonly used communications method within cloud environments to secure data in transit?

A. IPSec
B. HTTPS
C. VPN
D. DNSSEC

Answer: D

Explanation:
DNSSEC is used as a security extension to DNS lookup queries in order to ensure the authenticity and authoritativeness of hostname resolutions, in order to prevent spoofing and redirection of traffic. Although it is a very important concept to be employed for security practices, it is not used to secure or encrypt data transmissions. HTTPS is the most commonly used security mechanism for data communications between clients and websites and web services. IPSec is less commonly used, but is also intended to secure communications between servers. VPN is commonly used to secure traffic into a network area or subnet for developers and administrative users.

NEW QUESTION 80
- (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 82
- (Exam Topic 4)
Just like the risk management process, the BCDR planning process has a defined sequence of steps and processes to follow to ensure the production of a comprehensive and successful plan.
Which of the following is the correct sequence of steps for a BCDR plan?

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

Answer: A

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

NEW QUESTION 86
- (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 87
- (Exam Topic 4)
With a federated identity system, what does the identity provider send information to after a successful authentication?

A. Relying party
B. Service originator
C. Service relay

D. Service relay

Answer: A

Explanation:
Upon successful authentication, the identity provider sends an assertion with appropriate attributes to the relying party to grant access and assign appropriate roles to the user. The other terms provided are similar sounding to the correct term but are not actual components of a federated system.

NEW QUESTION 90
- (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 94
- (Exam Topic 4)
In the cloud motif, the data owner is usually:

A. The cloud provider
B. In another jurisdiction
C. The cloud customer
D. The cloud access security broker

Answer: C

Explanation:
The data owner is usually considered the cloud customer in a cloud configuration; the data in question is the customer's information, being processed in the cloud. The cloud provider is only leasing services and hardware to the customer. The cloud access security broker (CASB) only handles access control on behalf of the cloud customer, and is not in direct contact with the production data.

NEW QUESTION 96
- (Exam Topic 4)
There are many situations when testing a BCDR plan is appropriate or mandated. Which of the following would not be a necessary time to test a BCDR plan?

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

Answer: B

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

NEW QUESTION 99
- (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 103
- (Exam Topic 4)
BCDR strategies do not typically involve the entire operations of an organization, but only those deemed critical to their business.
Which concept pertains to the amount of services that need to be recovered to meet BCDR objectives?

A. RSL
B. RTO
C. RPO

D. SRE

Answer: A

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

NEW QUESTION 108
- (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 111
- (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 112
- (Exam Topic 4)
What is the concept of isolating an application from the underlying operating system for testing purposes?

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

Answer: B

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

NEW QUESTION 113
- (Exam Topic 4)
The BC/DR kit should include all of the following except:

A. Annotated asset inventory
B. Flashlight
C. Hard drives
D. Documentation equipment

Answer: C

Explanation:
While hard drives may be useful in the kit (for instance, if they store BC/DR data such as inventory lists, baselines, and patches), they are not necessarily required. All the other items should be included.

NEW QUESTION 118
- (Exam Topic 4)
Which of the following is a valid risk management metric?

A. KPI

B. KRI
C. SOC
D. SLA

Answer: B

Explanation:
KRI stands for key risk indicator. KRIs are the red flags if you will in the world of risk management. When these change, they indicate something is amiss and should be looked at quickly to determine if the change is minor or indicative of something important.

NEW QUESTION 120
- (Exam Topic 4)
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 125
- (Exam Topic 3)
Which of the following aspects of security is solely the responsibility of the cloud provider?

A. Regulatory compliance
B. Physical security
C. Operating system auditing
D. Personal security of developers

Answer: B

Explanation:
Regardless of the particular cloud service used, physical security of hardware and facilities is always the sole responsibility of the cloud provider. The cloud provider may release information about their physical security policies and procedures to ensure any particular requirements of potential customers will meet their regulatory obligations. Personal security of developers and regulatory compliance are always the responsibility of the cloud customer. Responsibility for operating systems, and the auditing of them, will differ based on the cloud service category used.

NEW QUESTION 127
- (Exam Topic 3)
The REST API is a widely used standard for communications of web-based services between clients and the servers hosting them.
Which protocol does the REST API depend on?

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

Answer: A

Explanation:
Representational State Transfer (REST) is a software architectural scheme that applies the components, connectors, and data conduits for many web applications used on the Internet. It uses and relies on the HTTP protocol and supports a variety of data formats. 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. Secure Shell client (SSH) is a secure method for allowing remote login to systems over a network.

NEW QUESTION 131
- (Exam Topic 3)
Where is a DLP solution generally installed when utilized for monitoring data in transit?

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

Answer: A

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

NEW QUESTION 134
- (Exam Topic 3)

With finite resources available within a cloud, even the largest cloud providers will at times need to determine which customers will receive additional resources first.
What is the term associated with this determination?

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

Answer: C

Explanation:
Shares are used within a cloud environment to prioritize resource allocation when customer requests exceed the available resources. Cloud providers utilize shares by assigning a priority score to each customer and allocating resources to those with the highest scores first. Scoring is a component of shares that determines the actual order in which to allocate resources. Neither weighting nor prioritization is the correct term in this case.

NEW QUESTION 137
- (Exam Topic 3)
Which of the following threat types can occur when baselines are not appropriately applied or when unauthorized changes are made?

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

Answer: A

Explanation:
Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner. This can be due to a shortcoming in security baselines or configurations, unauthorized changes to system configurations, or a failure to patch and upgrade systems as the vendor releases security patches. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. 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 or phishing attacks. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data.

NEW QUESTION 138
- (Exam Topic 3)
A DLP solution/implementation has three main components. Which of the following is NOT one of the three main components?

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

Answer: C

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

NEW QUESTION 140
- (Exam Topic 3)
During which phase of the cloud data lifecycle is it possible for the classification of data to change?

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

Answer: C

Explanation:
The create phase encompasses any time data is created, imported, or modified. With any change in the content or value of data, the classification may also change. It must be continually reevaluated to ensure proper security. During the use, share, and archive phases, the data is not modified in any way, so the original classification is still relevant.

NEW QUESTION 142
- (Exam Topic 3)
Which cloud deployment model would be ideal for a group of universities looking to work together, where each university can gain benefits according to its specific needs?

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

Answer: D

Explanation:
A community cloud is owned and maintained by similar organizations working toward a common goal. In this case, the universities would all have very similar needs and calendar requirements, and they would not be financial competitors of each other. Therefore, this would be an ideal group for working together within a community cloud. A public cloud model would not work in this scenario because it is designed to serve the largest number of customers, would not likely be targeted toward specific requirements for individual customers, and would not be willing to make changes for them. A private cloud could accommodate such needs, but would not meet the criteria for a group working together, and a hybrid cloud spanning multiple cloud providers would not fit the specifics of the question.

NEW QUESTION 145
- (Exam Topic 3)
Within a federated identity system, which entity accepts tokens from the identity provider?

A. Assertion manager
B. Servicing party
C. Proxy party
D. Relying party

Answer: D

Explanation:
The relying party is attached to the application or service that a user is trying to access, and it accepts authentication tokens from the user's own identity provider in order to facilitate authentication and access. The other terms provided are all associated with federated systems, but none is the correct choice in this case.

NEW QUESTION 148
- (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 149
- (Exam Topic 3)
Which cloud storage type requires special consideration on the part of the cloud customer to ensure they do not program themselves into a vendor lock-in situation?

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

Answer: D

Explanation:
Structured storage is designed, maintained, and implemented by a cloud service provider as part of a PaaS offering. It is specific to that cloud provider and the way they have opted to implement systems, so special care is required to ensure that applications are not designed in a way that will lock the cloud customer into a specific cloud provider with that dependency. Unstructured storage for auxiliary files would not lock a customer into a specific provider. With volume and object storage, because the cloud customer maintains their own systems with IaaS, moving and replicating to a different cloud provider would be very easy.

NEW QUESTION 152
- (Exam Topic 3)
Many of the traditional concepts of systems and services for a traditional data center also apply to the cloud. Both are built around key computing concepts.
Which of the following compromise the two facets of computing?

A. CPU and software
B. CPU and storage
C. CPU and memory
D. Memory and networking

Answer: C

Explanation:
The CPU and memory resources of an environment together comprise its "computing" resources. Cloud environments, especially public clouds, are enormous pools of resources for computing and are typically divided among a large number of customers with constantly changing needs and demands. Although storage and networking are core components of a cloud environment, they do not comprise its computing core. Software, much like within a traditional data center, is highly subjective based on the application, system, service, or cloud computing model used; however, it is not one of the core cloud components.

NEW QUESTION 155
- (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 160
- (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 163
4 to 80.6 degrees Fahrenheit (or 18 to 27 degrees Celsius) as the optimal temperature range for data centers. None of these options is the recommendation from ASHRAE.

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 166
- (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 168
- (Exam Topic 3)
Where is a DLP solution generally installed when utilized for monitoring data at rest?

A. Network firewall
B. Host system
C. Application server
D. Database server

Answer: B

Explanation:
To monitor data at rest appropriately, the DLP solution would be installed on the host system where the data resides. A database server, in some situations, may be an appropriate answer, but the host system is the best answer because a database server is only one example of where data could reside. An application server processes data and typically sits between the data and presentation zones, and as such, does not store data at rest. A network firewall would be more appropriate for data in transit because it is not a place where data would reside.

NEW QUESTION 170
- (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 172
- (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 177
- (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 178
- (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 181
- (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 186
- (Exam Topic 3)
Many tools and technologies are available for securing or monitoring data in transit within a data center, whether it is a traditional data center or a cloud. Which of the following is NOT a technology for securing data in transit?

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

Answer: C

Explanation:
DNSSEC is an extension of the normal DNS protocol that enables a system to verify the integrity of a DNS query resolution by signing it from the authoritative source and verifying the signing chain. It is not used for
securing data transmissions or exchanges. HTTPS is the most common method for securing web service and data calls within a cloud, and TLS is the current standard for encrypting HTTPS traffic. VPNs are widely used for securing data transmissions and service access.

NEW QUESTION 189
- (Exam Topic 3)
Which cloud storage type resembles a virtual hard drive and can be utilized in the same manner and with the same type of features and capabilities?

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

Answer: A

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

NEW QUESTION 194
- (Exam Topic 3)
If you are running an application that has strict legal requirements that the data cannot reside on systems that contain other applications or systems, which aspect of cloud computing would be prohibitive in this case?

A. Multitenancy
B. Broad network access
C. Portability
D. Elasticity

Answer: A

Explanation:
Multitenancy is the aspect of cloud computing that involves having multiple customers and applications running within the same system and sharing the same resources. Although considerable mechanisms are in place to ensure isolation and separation, the data and applications are ultimately using shared resources. Broad network access refers to the ability to access cloud services from any location or client. Portability refers to the ability to easily move cloud services between different cloud providers, whereas elasticity refers to the capabilities of a cloud environment to add or remove services, as needed, to meet current demand.

NEW QUESTION 195
- (Exam Topic 2)
Which of the cloud deployment models involves spanning multiple cloud environments or a mix of cloud hosting models?

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

Answer: C

Explanation:
A hybrid cloud model involves the use of more than one type of cloud hosting models, typically the mix of private and public cloud hosting models.

NEW QUESTION 198
- (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 199
- (Exam Topic 2)
Which aspect of cloud computing makes it very difficult to perform repeat audits over time to track changes and compliance?

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

Answer: A

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

NEW QUESTION 204
- (Exam Topic 2)
Which of the following is NOT a key area for performance monitoring as far as an SLA is concerned?

A. CPU
B. Users
C. Memory
D. Network

Answer: B

Explanation:
An SLA requires performance monitoring of CPU, memory, storage, and networking. The number of users active on a system would not be part of an SLA specifically, other than in regard to the impact on the other four variables.

NEW QUESTION 209
- (Exam Topic 2)
Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?

A. Infrastructure
B. Platform
C. Application
D. Data

Answer: D

Explanation:
Regardless of which cloud-hosting model is used, the cloud customer always has sole responsibility for the data and its security.

NEW QUESTION 210
- (Exam Topic 2)
What process is used within a cloud environment to maintain resource balancing and ensure that resources are available where and when needed?

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

Answer: D

Explanation:
Dynamic optimization is the process through which the cloud environment is constantly maintained to ensure resources are available when and where needed, and that physical nodes do not become overloaded or near capacity, while others are underutilized.

NEW QUESTION 212
- (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 215
- (Exam Topic 2)
Which type of controls are the SOC Type 1 reports specifically focused on?

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

Answer: C

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

NEW QUESTION 220
- (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 224
- (Exam Topic 2)
Over time, what is a primary concern for data archiving?

A. Size of archives
B. Format of archives
C. Recoverability
D. Regulatory changes

Answer: C

Explanation:
Over time, maintaining the ability to restore and read archives is a primary concern for data archiving. As technologies change and new systems are brought in, it is imperative for an organization to ensure they are still able to restore and access archives for the duration of the required retention period.

NEW QUESTION 226
- (Exam Topic 2)
Which of the following would be a reason to undertake a BCDR test?

A. Functional change of the application
B. Change in staff
C. User interface overhaul of the application
D. Change in regulations

Answer: A

Explanation:
Any time a major functional change of an application occurs, a new BCDR test should be done to ensure the overall strategy and process are still applicable and appropriate.

NEW QUESTION 227
- (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 229
- (Exam Topic 2)
Which entity requires all collection and storing of data on their citizens to be done on hardware that resides within their borders?

A. Russia
B. France
C. Germany
D. United States

Answer: A

Explanation:
Signed into law and effective starting on September 1, 2015, Russian Law 526-FZ establishes that any collecting, storing, or processing of personal information or data on Russian citizens must be done from systems and databases that are physically located with the Russian Federation.

NEW QUESTION 230
- (Exam Topic 2)
Which of the following should NOT be part of the requirement analysis phase of the software development lifecycle?

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

Answer: D

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

NEW QUESTION 234
- (Exam Topic 2)
Which of the following would NOT be a reason to activate a BCDR strategy?

A. Staffing loss
B. Terrorism attack
C. Utility disruptions
D. Natural disaster

Answer: A

Explanation:
The loss of staffing would not be a reason to declare a BCDR situation because it does not impact production operations or equipment, and the same staff would be needed for a BCDR situation.

NEW QUESTION 238
- (Exam Topic 2)
Which security concept would business continuity and disaster recovery fall under?

A. Confidentiality
B. Availability
C. Fault tolerance
D. Integrity

Answer: B

Explanation:
Disaster recovery and business continuity are vital concerns with availability. If data is destroyed or compromised, having regular backup systems in place as well as being able to perform disaster recovery in the event of a major or widespread problem allows operations to continue with an acceptable loss of time and data to management. This also ensures that sensitive data is protected and persisted in the event of the loss or corruption of data systems or physical storage systems.

NEW QUESTION 241
- (Exam Topic 1)
What is the biggest concern with hosting a key management system outside of the cloud environment?

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

Answer: C

Explanation:
When a key management system is outside of the cloud environment hosting the application, availability is a primary concern because any access issues with the encryption keys will render the entire application unusable.

NEW QUESTION 245
- (Exam Topic 1)
Which publication from the United States National Institute of Standards and Technology pertains to defining cloud concepts and definitions for the various core components of cloud computing?

A. SP 800-153
B. SP 800-145
C. SP 800-53
D. SP 800-40

Answer: B

Explanation:
NIST Special Publications 800-145 is titled "The NIST Definition of Cloud Computing" and contains definitions and explanations of core cloud concepts and components.

NEW QUESTION 250
- (Exam Topic 1)
Which of the following threat types can occur when baselines are not appropriately applied or unauthorized changes are made?

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

Answer: C

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

NEW QUESTION 253
- (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 255
- (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 257
- (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 258
- (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 259
- (Exam Topic 1)
Which technology is NOT commonly used for security with data in transit?

A. DNSSEC
B. IPsec
C. VPN
D. HTTPS

Answer: A

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

NEW QUESTION 260
- (Exam Topic 1)
Which of the following pertains to fire safety standards within a data center, specifically with their enormous electrical consumption?

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

Answer: A

Explanation:
The standards put out by the National Fire Protection Association (NFPA) cover general fire protection best practices for any type of facility, but also specific publications pertaining to IT equipment and data centers.

NEW QUESTION 262
- (Exam Topic 1)
Which of the following does NOT relate to the hiding of sensitive data from data sets?

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

Answer: B

Explanation:
Federation pertains to authenticating systems between different organizations.

NEW QUESTION 265
- (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 266
- (Exam Topic 1)
Which jurisdiction lacks specific and comprehensive privacy laws at a national or top level of legal authority?

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

Answer: D

Explanation:
The United States lacks a single comprehensive law at the federal level addressing data security and privacy, but there are multiple federal laws that deal with different industries.

NEW QUESTION 271
- (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 274
- (Exam Topic 1)
Which of the following threat types can occur when encryption is not properly applied or insecure transport mechanisms are used?

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

Answer: C

Explanation:
Sensitive data exposure occurs when information is not properly secured through encryption and secure transport mechanisms; it can quickly become an easy and broad method for attackers to compromise information. Web applications must enforce strong encryption and security controls on the application side, but secure methods of communications with browsers or other clients used to access the information are also required. Security misconfiguration occurs when applications and systems are not properly configured for security, often a result of misapplied or inadequate baselines. Insecure direct object references occur when code references aspects of the infrastructure, especially internal or private systems, and an attacker can use that knowledge to glean more information about the infrastructure. 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, thus allowing spoofing for malware or phishing attacks.

NEW QUESTION 278
- (Exam Topic 1)
Which of the following are the storage types associated with PaaS?

A. Structured and freeform
B. Volume and object
C. Structured and unstructured
D. Database and file system

Answer: C

NEW QUESTION 279
- (Exam Topic 1)
Which United States law is focused on data related to health records and privacy?

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

Answer: D

Explanation:
The Health Insurance Portability and Accountability Act (HIPAA) requires the U.S. Federal Department of Health and Human Services to publish and enforce regulations pertaining to electronic health records and identifiers between patients, providers, and insurance companies. It is focused on the security controls and confidentiality of medical records, rather than the specific technologies used, so long as they meet the requirements of the regulations.

NEW QUESTION 281

- (Exam Topic 1)
What is the best approach for dealing with services or utilities that are installed on a system but not needed to perform their desired function?

A. Remove
B. Monitor
C. Disable
D. Stop

Answer: A

Explanation:
The best practice is to totally remove any unneeded services and utilities on a system to prevent any chance of compromise or use. If they are just disabled, it is possible for them to be inadvertently started again at any point, or another exploit could be used to start them again. Removing also negates the need to patch and maintain them going forward.

NEW QUESTION 282
- (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 286
- (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 290
- (Exam Topic 1)
What must be secured on physical hardware to prevent unauthorized access to systems?

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

Answer: A

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

NEW QUESTION 295
......