# ISC.CCSP.v2022-02-04.q267

| | |
|---|---|
| **Exam Code:** | CCSP |
| **Exam Name:** | Certified Cloud Security Professional |
| **Certification Provider:** | ISC |
| **Free Question Number:** | 267 |
| **Version:** | v2022-02-04 |
| **# of views:** | 5005 |
| **# of Questions views:** | 2670 |
| https://www.exam-tests.com/CCSP-exam/ISC.CCSP.v2022-02-04.q267.html | |

**NEW QUESTION: 1**
GAAPs are created and maintained by which organization?
**A.** ISO/IEC
**B.** AICPA
**C.** PCI Council
**D.** ISO
**Answer: B (LEAVE A REPLY)**
The AICPA is the organization responsible for generating and maintaining what are the Generally Accepted Accounting Practices in the United States.

**NEW QUESTION: 2**
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 (LEAVE A REPLY)**
Explanation
Background checks are controls for attenuating potential threats from internal actors; external threats aren't likely to submit to background checks.

**NEW QUESTION: 3**
When using an IaaS solution, what is the capability provided to the customer?

**A.** To provision processing, storage, networks, and other fundamental computing resources when the consumer is able to deploy and run arbitrary software, which can include OSs and applications.
**B.** To provision processing, storage, networks, and other fundamental computing resources when the auditor is able to deploy and run arbitrary software, which can include OSs and applications.
**C.** To provision processing, storage, networks, and other fundamental computing resources when the provider is able to deploy and run arbitrary software, which can include OSs and applications.
**D.** To provision processing, storage, networks, and other fundamental computing resources when the consumer is not able to deploy and run arbitrary software, which can include OSs and applications.
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation:
According to "The NIST Definition of Cloud Computing," in IaaS, "the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

**NEW QUESTION: 4**
The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program has _____ tiers.
Response:
**A.** Two
**B.** Three
**C.** Four
**D.** Eight
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 5**
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 (LEAVE A REPLY)**

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: 6**
When using transparent encryption of a database, where does the encryption engine reside?
**A.** In a key management system
**B.** On the instance(s) attached to the volume
**C.** At the application using the database
**D.** Within the database
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 7**
The Cloud Security Alliance (CSA) publishes, the Notorious Nine, a list of common threats to organizations participating in cloud computing.
According to the CSA, all of the following activity can result in data loss except _____.
**A.** Misplaced crypto keys
**B.** Accidental overwrite
**C.** Improper policy
**D.** Ineffectual backup procedures
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 8**
Which of the following storage types is most closely associated with a traditional file system and tree structure?
**A.** Volume
**B.** Unstructured
**C.** Object
**D.** Structured
**Answer: (SHOW ANSWER)**
Explanation
Explanation:
Volume storage works as a virtual hard drive that is attached to a virtual machine. The operating system sees the volume the same as how a traditional drive on a physical server would be seen.

**NEW QUESTION: 9**
You are the security policy lead for your organization, which is considering migrating from your on- premises, legacy environment into the cloud. You are reviewing the Cloud

Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization. What is probably the best benefit offered by the CCM?
**A.** Allowing your organization to leverage existing controls across multiple frameworks so as not to duplicate effort
**B.** The low cost of the tool
**C.** Simplicity of control selection from the list of approved choices
**D.** Ease of implementation by choosing controls from the list of qualified vendors
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 10**
Which protocol does the REST API depend on?
**A.** HTTP
**B.** XML
**C.** SAML
**D.** SSH
**Answer: A (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
Representational State Transfer (REST) is a software architectural scheme that applies the components, connectors, and data conduits for many web applications used on the Internet. It uses and relies on the HTTP protocol and supports a variety of data formats.

**NEW QUESTION: 11**
What is the biggest challenge to data discovery in a cloud environment?
**A.** Format
**B.** Ownership
**C.** Location
**D.** Multitenancy
**Answer: (SHOW ANSWER)**
Explanation/Reference:
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: 12**
DLP can be combined with what other security technology to enhance data controls?
**A.** SIEM
**B.** Hypervisors
**C.** DRM
**D.** Kerberos

**Answer: C (LEAVE A REPLY)**
Explanation
DLP can be combined with DRM to protect intellectual property; both are designed to deal with data that falls into special categories. SIEMs are used for monitoring event logs, not live data movement. Kerberos is an authentication mechanism. Hypervisors are used for virtualization.

**NEW QUESTION: 13**
All policies within the organization should include a section that includes all of the following, except:
**A.** Policy review
**B.** Policy adjudication
**C.** Policy maintenance
**D.** Policy enforcement
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 14**
Although much of the attention given to data security is focused on keeping data private and only accessible by authorized individuals, of equal importance is the trustworthiness of the data.
Which concept encapsulates this?
**A.** Validity
**B.** Integrity
**C.** Accessibility
**D.** Confidentiality
**Answer: (SHOW ANSWER)**
Explanation
Integrity refers to the trustworthiness of data and whether its format and values are true and have not been corrupted or otherwise altered through unauthorized means.
Confidentiality refers to keeping data from being access or viewed by unauthorized parties.
Accessibility means that data is available and ready when needed by a user or service.
Validity can mean a variety of things that are somewhat similar to integrity, but it's not the most appropriate answer in this case.

**NEW QUESTION: 15**
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months.
The 2013 OWASP Top Ten list includes "cross- site scripting (XSS)."
Which of the following is not a method for reducing the risk of XSS attacks?
**A.** Use an auto-escaping template system.

**B.** Sanitize HTML markup with a library designed for the purpose.
**C.** XML escape all identity assertions.
**D.** HTML escape JSON values in an HTML context and read the data with JSON.parse.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 16**
If a cloud computing customer wishes to guarantee that a minimum level of resources will always be available, which of the following set of services would compromise the reservation?
**A.** Memory and networking
**B.** CPU and software
**C.** CPU and storage
**D.** CPU and memory
**Answer: D (LEAVE A REPLY)**
A reservation guarantees to a cloud customer that they will have access to a minimal level of resources to run their systems, which will help mitigate against DoS attacks or systems that consume high levels of resources. A reservation pertains to memory and CPU resources. Under the concept of a reservation, memory and CPU are the guaranteed resources, but storage and networking are not included even though they are core components of cloud computing. Software would be out of scope for a guarantee and doesn't really pertain to the concept.



**NEW QUESTION: 17**
Which of the following contract terms most incentivizes the cloud provider to meet the requirements listed in the SLA?
**A.** Regulatory oversight
**B.** Financial penalties
**C.** Desire to maintain customer satisfaction
**D.** Performance details
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 18**

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: (SHOW ANSWER)**
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: 19**
Which type of testing tends to produce the best and most comprehensive results for discovering system vulnerabilities?
**A.** Vulnerability
**B.** Static
**C.** Pen
**D.** Dynamic
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 20**
Which of the following is the optimal temperature for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?
**A.** 69.8-86.0degF (21-30degC)
**B.** 64.4-80.6degF(18-27degC)
**C.** 51.8-66.2degF(11-19degC)
**D.** 44.6-60-8degF(7-16degC)
**Answer: B (LEAVE A REPLY)**
The guidelines from ASHRAE establish 64.4-80.6degF (18-27degC) as the optimal temperature for a data center.

**NEW QUESTION: 21**
All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline except _____.
**A.** Include the baseline image in the asset inventory/configuration management database
**B.** Configure the host OS according to the baseline requirements

**C.** Exclude the target system you intend to baseline from any scheduled updates/patching used in production systems
**D.** Remove all nonessential programs from the baseline image
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 22**
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 (LEAVE A REPLY)**
Explanation/Reference:
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: 23**
Which of the following are the storage types associated with IaaS?
**A.** Volume and container
**B.** Volume and label
**C.** Object and target
**D.** Volume and object
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 24**
The physical layout of a cloud data center campus should include redundancies of all the following except
_____.
Response:
**A.** Electrical utility lines
**B.** Physical perimeter security controls (fences, lights, walls, etc.)
**C.** Communications connectivity lines
**D.** The administration/support staff building
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 25**
What is the primary security mechanism used to protect SOAP and REST APIs?
Response:
**A.** XML firewalls

**B.** WAFs
**C.** Encryption
**D.** Firewalls
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 26**
Which security concept would business continuity and disaster recovery fall under?
**A.** Confidentiality
**B.** Availability
**C.** Fault tolerance
**D.** Integrity
**Answer: (SHOW ANSWER)**
Explanation/Reference:
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: 27**
Before deploying a specific brand of virtualization toolset, it is important to configure it according to _____.
**A.** Expert opinion
**B.** Prevailing law of that jurisdiction
**C.** Industry standards
**D.** Vendor guidance
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 28**
Which of the following may unilaterally deem a cloud hosting model inappropriate for a system or application?
**A.** Multitenancy
**B.** Certification
**C.** Regulation
**D.** Virtualization
**Answer: C (LEAVE A REPLY)**
Explanation/Reference:
Explanation:

Some regulations may require specific security controls or certifications be used for hosting certain types of data or functions, and in some circumstances they may be requirements that are unable to be met by any cloud provider.

**NEW QUESTION: 29**
Which type of cloud model typically presents the most challenges to a cloud customer during the "destroy" phase of the cloud data lifecycle?
**A.** IaaS
**B.** DaaS
**C.** SaaS
**D.** PaaS
**Answer: C (LEAVE A REPLY)**
Explanation
With many SaaS implementations, data is not isolated to a particular customer but rather is part of the overall application. When it comes to data destruction, a particular challenge is ensuring that all of a customer's data is completely destroyed while not impacting the data of other customers.

**NEW QUESTION: 30**
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 (LEAVE A REPLY)**
Explanation
DoS/DDoS threats and risks are not unique to the public cloud model.

**NEW QUESTION: 31**
An SLA contains the official requirements for contract performance and satisfaction between the cloud provider and cloud customer.
Which of the following would NOT be a component with measurable metrics and requirements as part of an SLA?
**A.** Network
**B.** Users
**C.** Memory
**D.** CPU
**Answer: B (LEAVE A REPLY)**
Dealing with users or user access would not be an appropriate item for inclusion in an SLA specifically.

However, user access and user experience would be covered indirectly through other metrics. Memory, CPU, and network resources are all typically included within an SLA for availability and response times when dealing with any incidents.



**NEW QUESTION: 32**
What sort of legal enforcement may the Payment Card Industry (PCI) Security Standards Council not bring to bear against organizations that fail to comply with the Payment Card Industry Data Security Standard (PCI DSS)?
**A.** Subject to increased audit frequency and scope
**B.** Suspension of credit card processing privileges
**C.** Jail time
**D.** Fines
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 33**
What concept does the "R" represent with the DREAD model?
**A.** Reproducibility
**B.** Repudiation
**C.** Risk
**D.** Residual
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation:
Reproducibility is the measure of how easy it is to reproduce and successful use an exploit. Scoring within the DREAD model ranges from 0, signifying a nearly impossibly exploit, up to 10, which signifies something that anyone from a simple function call could exploit, such as a URL.

**NEW QUESTION: 34**
Which component of ITIL involves handling anything that can impact services for either internal or public users?
**A.** Incident management

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

**NEW QUESTION: 35**
What is the intellectual property protection for the logo of a new video game?
Response:
**A.** Trademark
**B.** Patent
**C.** Copyright
**D.** Trade secret
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 36**
All of the following might be used as data discovery characteristics in a content-analysis-based data discovery effort except _____.
Response:
**A.** Keywords
**B.** Frequency
**C.** Pattern-matching
**D.** Inheritance
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 37**
The BIA can be used to provide information about all the following, except:
**A.** BC/DR planning
**B.** Risk analysis
**C.** Secure acquisition
**D.** Selection of security controls
**Answer: (SHOW ANSWER)**

Explanation
The business impact analysis gathers asset valuation information that is beneficial for risk analysis and selection of security controls (it helps avoid putting the ten-dollar lock on the five-dollar bicycle), and criticality information that helps in BC/DR planning by letting the organization understand which systems, data, and personnel are necessary to continuously maintain. However, it does not aid secure acquisition efforts, since the assets examined by the BIA have already been acquired.

**NEW QUESTION: 38**
Which of the following standards primarily pertains to cabling designs and setups in a data center?
**A.** IDCA
**B.** BICSI
**C.** NFPA
**D.** Uptime Institute
**Answer: B (LEAVE A REPLY)**
Explanation
The standards put out by Building Industry Consulting Service International (BICSI) primarily cover complex cabling designs and setups for data centers, but also include specifications on power, energy efficiency, and hot/cold aisle setups.

**NEW QUESTION: 39**
When an organization is considering the use of cloud services for BCDR planning and solutions, which of the following cloud concepts would be the most important?
**A.** Reversibility
**B.** Elasticity
**C.** Interoperability
**D.** Portability
**Answer: D (LEAVE A REPLY)**
Portability is the ability for a service or system to easily move among different cloud providers. This is essential for using a cloud solution for BCDR because vendor lock-in would inhibit easily moving and setting up services in the event of a disaster, or it would necessitate a large number of configuration or component changes to implement. Interoperability, or the ability to reuse components for other services or systems, would not be an important factor for BCDR. Reversibility, or the ability to remove all data quickly and completely from a cloud environment, would be important at the end of a disaster, but would not be important during setup and deployment. Elasticity, or the ability to resize resources to meet current demand, would be very beneficial to a BCDR situation, but not as vital as portability.

**NEW QUESTION: 40**

What concept does the "R" represent with the DREAD model?
**A.** Reproducibility
**B.** Repudiation
**C.** Risk
**D.** Residual
**Answer: A (LEAVE A REPLY)**
Reproducibility is the measure of how easy it is to reproduce and successful use an exploit. Scoring within the DREAD model ranges from 0, signifying a nearly impossibly exploit, up to 10, which signifies something that anyone from a simple function call could exploit, such as a URL.

**NEW QUESTION: 41**
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 (LEAVE A REPLY)**
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: 42**
Which of the following are attributes of cloud computing?
**A.** Minimal management effort and shared resources
**B.** High cost and unique resources
**C.** Rapid provisioning and slow release of resources
**D.** Limited access and service provider interaction
**Answer: A (LEAVE A REPLY)**
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

**NEW QUESTION: 43**
Data labels could include all the following, except:

**A.** Multifactor authentication
**B.** Access restrictions
**C.** Confidentiality level
**D.** Distribution limitations
**Answer: A (LEAVE A REPLY)**
Explanation
All the others might be included in data labels, but multifactor authentication is a procedure used for access control, not a label.

**NEW QUESTION: 44**
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: (SHOW ANSWER)**
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: 45**
Clustered systems can be used to ensure high availability and load balancing across individual systems through a variety of methodologies.
What process is used within a clustered system to ensure proper load balancing and to maintain the health of the overall system to provide high availability?
**A.** Distributed clustering
**B.** Distributed balancing
**C.** Distributed optimization
**D.** Distributed resource scheduling
**Answer: (SHOW ANSWER)**
Distributed resource scheduling (DRS) is used within all clustered systems as the method for providing high availability, scaling, management, workload distribution, and the balancing of jobs and processes. None of the other choices is the correct term in this case.

**NEW QUESTION: 46**
What aspect of data center planning occurs first?
Response:
**A.** Audit
**B.** Policy revision

**C.** Logical design
**D.** Physical design
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 47**
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
In order to get truly holistic coverage of your environment, you should be sure to include _____ as a step in the deployment process.
**A.** All of your customers to install the tool
**B.** Getting signed user agreements from all users
**C.** Adoption of the tool in all routers between your users and the cloud provider
**D.** Installation of the solution on all assets in the cloud data center
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 48**
Different types of cloud deployment models use different types of storage from traditional data centers, along with many new types of software platforms for deploying applications and configurations. Which of the following is NOT a storage type used within a cloud environment?
**A.** Structured
**B.** Volume
**C.** Object
**D.** Docker
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 49**
Data centers have enormous power resources that are distributed and consumed throughout the entire facility.
Which of the following standards pertains to the proper fire safety standards within that scope?
**A.** IDCA

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

**NEW QUESTION: 50**
Which of the following practices can enhance both operational capabilities and configuration management efforts?
**A.** Constant uptime
**B.** Multifactor authentication
**C.** File hashes
**D.** Regular backups
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 51**
The use of which of the following technologies will NOT require the security dependency of an operating system, other than its own?
**A.** Type 1 hypervisor
**B.** Type 2 hypervisor
**C.** Management plane
**D.** Virtual machine
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 52**
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: (SHOW ANSWER)**
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: 53**
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 (LEAVE A REPLY)**
Explanation/Reference:
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: 54**
Which of the following standards primarily pertains to cabling designs and setups in a data center?
**A.** IDCA
**B.** BICSI
**C.** NFPA
**D.** Uptime Institute
**Answer: B (LEAVE A REPLY)**
The standards put out by Building Industry Consulting Service International (BICSI) primarily cover complex cabling designs and setups for data centers, but also include specifications on power, energy efficiency, and hot/cold aisle setups.

**NEW QUESTION: 55**
Which document will enforce uptime and availability requirements between the cloud customer and cloud provider?
Response:
**A.** Contract
**B.** Operational level agreement
**C.** Regulation
**D.** Service level agreement
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 56**

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 (LEAVE A REPLY)**

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

**NEW QUESTION: 57**

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 (LEAVE A REPLY)**

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: 58**

What can tokenization be used for?

Response:

**A.** Encryption

**B.** Compliance with PCI DSS

**C.** Giving management oversight to e-commerce functions

**D.** Enhancing the user experience

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 59**

You are the IT security manager for a video game software development company. Which of the following is most likely to be your primary concern on a daily basis?

Response:

**A.** Health and human safety

**B.** Security flaws in your products

**C.** Security flaws in your organization

**D.** Regulatory compliance

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 60**
What type of segregation and separation of resources is needed within a cloud environment for multitenancy purposes versus a traditional data center model?
**A.** Virtual
**B.** Security
**C.** Physical
**D.** Logical
**Answer: D (LEAVE A REPLY)**
Explanation
Cloud environments lack the ability to physically separate resources like a traditional data center can. To compensate, cloud computing logical segregation concepts are employed. These include VLANs, sandboxing, and the use of virtual network devices such as firewalls.

**NEW QUESTION: 61**
A cloud data encryption situation where the cloud customer retains control of the encryption keys and the cloud provider only processes and stores the data could be considered a _____.
Response:
**A.** Threat
**B.** Risk
**C.** Hybrid cloud deployment model
**D.** Case of infringing on the rights of the provider
**Answer: C (LEAVE A REPLY)**



**NEW QUESTION: 62**
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 (LEAVE A REPLY)**

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: 63**

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 (LEAVE A REPLY)**

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: 64**

Which cloud service category is MOST likely to use a client-side key management system?

**A.** DaaS

**B.** SaaS

**C.** PaaS

**D.** IaaS

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 65**

Which type of audit report does many cloud providers use to instill confidence in their policies, practices, and procedures to current and potential customers?

**A.** SAS-70

**B.** SOC 2

**C.** SOC 1
**D.** SOX
**Answer: B (LEAVE A REPLY)**
One approach that many cloud providers opt to take is to undergo a SOC 2 audit and make the report available to cloud customers and potential cloud customers as a way of providing security confidence without having to open their systems or sensitive information to the masses.

**NEW QUESTION: 66**
Where is an XML firewall most commonly and effectively deployed in the environment?
**A.** Between the application and data layers
**B.** Between the presentation and application layers
**C.** Between the IPS and firewall
**D.** Between the firewall and application server
**Answer: D (LEAVE A REPLY)**
An XML firewall is most commonly deployed in line between the firewall and application server to validate XML code before it reaches the application. An XML firewall is intended to validate XML before it reaches the application. Placing the XML firewall between the presentation and application layers, between the firewall and IPS, or between the application and data layers would not serve the intended purpose.

**NEW QUESTION: 67**
You need to gain approval to begin moving your company's data and systems into a cloud environment.
However, your CEO has mandated the ability to easily remove your IT assets from the cloud provider as a precondition.
Which of the following cloud concepts would this pertain to?
**A.** Removability
**B.** Extraction
**C.** Portability
**D.** Reversibility
**Answer: D (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
Reversibility is the cloud concept involving the ability for a cloud customer to remove all of its data and IT assets from a cloud provider. Also, processes and agreements would be in place with the cloud provider that ensure all removals have been completed fully within the agreed upon timeframe. Portability refers to the ability to easily move between different cloud providers and not be locked into a specific one.
Removability and extraction are both provided as terms similar to reversibility, but neither is the official term or concept.

**NEW QUESTION: 68**
The Brewer-Nash security model is also known as which of the following?
Response:
**A.** MAC
**B.** RBAC
**C.** Preventive measures
**D.** The Chinese Wall model
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 69**
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 (LEAVE A REPLY)**
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: 70**
Which European Union directive pertains to personal data privacy and an individual's control over their personal data?
**A.** 99/9/EC
**B.** 95/46/EC
**C.** 2000/1/EC
**D.** 2013/27001/EC
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation:
Directive 95/46/EC is titled "On the protection of individuals with regard to the processing of personal data and on the free movement of such data."

**NEW QUESTION: 71**
What concept does the "D" represent with the STRIDE threat model?
**A.** Data loss
**B.** Denial of service
**C.** Data breach
**D.** Distributed

**Answer: (SHOW ANSWER)**
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: 72**
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 (LEAVE A REPLY)**
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: 73**
Every security program and process should have which of the following?
**A.** Severe penalties
**B.** Multifactor authentication
**C.** Foundational policy
**D.** Homomorphic encryption
**Answer: (SHOW ANSWER)**
Explanation
Policy drives all programs and functions in the organization; the organization should not conduct any operations that don't have a policy governing them. Penalties may or may not be an element of policy, and severity depends on the topic. Multifactor authentication and homomorphic encryption are red herrings here.

**NEW QUESTION: 74**

Which of the following is NOT one of the cloud computing activities, as outlined in ISO/IEC 17789?
Response:
**A.** Cloud service provider
**B.** Cloud service partner
**C.** Cloud service customer
**D.** Cloud service administrator
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 75**
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 an overview of application security that introduces definitive concepts, principles, and processes involved in application security.
**D.** Provides on overview of network and infrastructure security designed to secure cloud applications.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 76**
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: (SHOW ANSWER)**
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: 77**
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 (LEAVE A REPLY)**
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: 78**
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: (SHOW ANSWER)**
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: 79**
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: (SHOW ANSWER)**
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: 80**
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: (SHOW ANSWER)**
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: 81**
SOX was enacted because of which of the following?
Response:
**A.** Poor BOD oversight
**B.** Lack of independent audits
**C.** Poor financial controls
**D.** All of the above
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 82**
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 (LEAVE A REPLY)**
Explanation/Reference:
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: 83**
Data transformation in a cloud environment should be of great concern to organizations considering cloud migration because _____ could affect data classification processes/implementations.
**A.** Physical distance
**B.** Multitenancy
**C.** Virtualization
**D.** Remote access
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 84**
Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?
Response:
**A.** Unvalidated redirects and forwards
**B.** Cross-site request forgery
**C.** Insecure direct object references
**D.** Cross-site scripting
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 85**
What does SDN stand for within a cloud environment?
**A.** Software-dynamic networking
**B.** Software-defined networking

**C.** Software-dependent networking
**D.** System-dynamic nodes
**Answer: (SHOW ANSWER)**
Explanation
Software-defined networking separates the administration of network filtering and network forwarding to allow for distributed administration.

**NEW QUESTION: 86**
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 (LEAVE A REPLY)**
Explanation/Reference:
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: 87**
In which of the following situations does the data owner have to administer the OS?
Response:
**A.** PaaS
**B.** IaaS
**C.** Offsite archive
**D.** SaaS
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 88**
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 (LEAVE A REPLY)**

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: 89**
To protect data on user devices in a BYOD environment, the organization should consider requiring all the following, except:
**A.** Multifactor authentication
**B.** DLP agents
**C.** Two-person integrity
**D.** Local encryption
**Answer: C (LEAVE A REPLY)**
Explanation
Although all the other options are ways to harden a mobile device, two-person integrity is a concept that has nothing to do with the topic, and, if implemented, would require everyone in your organization to walk around in pairs while using their mobile devices.

**NEW QUESTION: 90**
You are a consultant performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost $24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant. The fire suppression system costs $15 million. An insurance policy that would cover the full replacement cost of the plant costs $1 million per month.
In order to establish the true annualized loss expectancy (ALE), you would need all of the following information except _____.
Response:
**A.** The length of time it would take to rebuild the plant
**B.** The amount of product the plant creates
**C.** The rate at which the plant generates revenue
**D.** The amount of revenue generated by the plant
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 91**
Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?
**A.** Regulation
**B.** Multitenancy
**C.** Virtualization
**D.** Resource pooling
**Answer: B (LEAVE A REPLY)**
Explanation

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



**NEW QUESTION: 92**
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: (SHOW ANSWER)**
Explanation/Reference:
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: 93**
All of the following entitles are required to use FedRAMP-accredited Cloud Service Providers except _____.
**A.** The CIA
**B.** The US post office
**C.** The Department of Homeland Security

**D.** Federal Express
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 94**
With a cloud service category where the cloud customer is responsible for deploying all services, systems, and components needed for their applications, which of the following storage types are MOST likely to be available to them?
**A.** Structured and hierarchical
**B.** Volume and object
**C.** Volume and database
**D.** Structured and unstructured
**Answer: B (LEAVE A REPLY)**
The question is describing the Infrastructure as a Service (IaaS) cloud offering, and as such, the volume and object storage types will be available to the customer. Structured and unstructured are storage types associated with PaaS, and although the other answers present similar- sounding storage types, they are a mix of real and fake names.

**NEW QUESTION: 95**
What is the concept of segregating information or processes, within the same system or application, for security reasons?
**A.** fencing
**B.** Sandboxing
**C.** Cellblocking
**D.** Pooling
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation:
Sandboxing involves segregating and isolating information or processes from others within the same system or application, typically for security concerns. This is generally used for data isolation (for example, keeping different communities and populations of users isolated from other similar data).

**NEW QUESTION: 96**
The management plane is used to administer a cloud environment and perform administrative tasks across a variety of systems, but most specifically it's used with the hypervisors.
What does the management plane typically leverage for this orchestration?
**A.** APIs
**B.** Scripts
**C.** TLS
**D.** XML

**Answer: A (LEAVE A REPLY)**
The management plane uses APIs to execute remote calls across the cloud environment to various management systems, especially hypervisors. This allows a centralized administrative interface, often a web portal, to orchestrate tasks throughout an enterprise. Scripts may be utilized to execute API calls, but they are not used directly to interact with systems. XML is used for data encoding and transmission, but not for executing remote calls. TLS is used to encrypt communications and may be used with API calls, but it is not the actual process for executing commands.

**NEW QUESTION: 97**
What sort of legal enforcement may the Payment Card Industry (PCI) Security Standards Council not bring to bear against organizations that fail to comply with the Payment Card Industry Data Security Standard (PCI DSS)?
Response:
**A.** Fines
**B.** Jail time
**C.** Subject to increased audit frequency and scope
**D.** Suspension of credit card processing privileges
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 98**
Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?
**A.** Hybrid
**B.** Public
**C.** Private
**D.** Community
**Answer: B (LEAVE A REPLY)**
Explanation
Popular services such as iCloud, Dropbox, and OneDrive are all publicly available and are open to any user for free, with possible add-on services offered for a cost.

**NEW QUESTION: 99**
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: (SHOW ANSWER)**

Explanation/Reference:
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: 100**
Which component of ITIL involves the creation of an RFC ticket and obtaining official approvals for it?
**A.** Problem management
**B.** Release management
**C.** Deployment management
**D.** Change management
**Answer: (SHOW ANSWER)**
The change management process involves the creation of the official Request for Change (RFC) ticket, which is used to document the change, obtain the required approvals from management and stakeholders, and track the change to completion. Release management is a subcomponent of change management, where the actual code or configuration change is put into place. Deployment management is similar to release management, but it's where changes are actually implemented on systems. Problem management is focused on the identification and mitigation of known problems and deficiencies before they are able to occur.

**NEW QUESTION: 101**
In a federated identity arrangement using a trusted third-party model, who is the identity provider and who is the relying party?
**A.** The users of the various organizations within the federations within the federation/a CASB
**B.** Each member organization/a trusted third party
**C.** Each member organization/each member organization
**D.** A contracted third party/the various member organizations of the federation
**Answer: D (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
In a trusted third-party model of federation, each member organization outsources the review and approval task to a third party they all trust. This makes the third party the identifier (it issues and manages identities for all users in all organizations in the

federation), and the various member organizations are the relying parties (the resource providers that share resources based on approval from the third party).

**NEW QUESTION: 102**
Which of the following best describes data masking?
**A.** A method for creating similar but inauthentic datasets used for software testing and user training.
**B.** A method used to protect prying eyes from data such as social security numbers and credit card data.
**C.** A method where the last few numbers in a dataset are not obscured. These are often used for authentication.
**D.** Data masking involves stripping out all digits in a string of numbers so as to obscure the original number.
**Answer: (SHOW ANSWER)**
All of these answers are actually correct, but A is the best answer, because it is the most general, includes the others, and is therefore the optimum choice. This is a good example of the type of question that can appear on the actual exam.

**NEW QUESTION: 103**
Which cloud service category most commonly uses client-side key management systems?
**A.** Software as a Service
**B.** Infrastructure as a Service
**C.** Platform as a Service
**D.** Desktop as a Service
**Answer: (SHOW ANSWER)**
SaaS most commonly uses client-side key management. With this type of implementation, the software for doing key management is supplied by the cloud provider, but is hosted and run by the cloud customer.
This allows for full integration with the SaaS implementation, but also provides full control to the cloud customer. Although the cloud provider may offer software for performing key management to the cloud customers, with the Infrastructure, Platform, and Desktop as a Service categories, the customers would largely be responsible for their own options and implementations and would not be bound by the offerings from the cloud provider.

**NEW QUESTION: 104**
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 (LEAVE A REPLY)**

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: 105**
Although encryption can help an organization to effectively decrease the possibility of data breaches, which other type of threat can it increase the chances of?
Response:
**A.** System vulnerabilities
**B.** Data loss
**C.** Insecure interfaces
**D.** Account hijacking
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 106**
What's a potential problem when object storage versus volume storage is used within IaaS for application use and dependency?
**A.** Object storage is only optimized for small files.
**B.** Object storage is its own system, and data consistency depends on replication.
**C.** Object storage may have availability issues.
**D.** Object storage is dependent on access control from the host server.
**Answer: B (LEAVE A REPLY)**
Explanation
Object storage runs on its own independent systems, which have their own redundancy and distribution. To ensure data consistency, sufficient time is needed for objects to fully replicate to all potential locations before being accessed. Object storage is optimized for high availability and will not be any less reliable than any other virtual machine within a cloud environment. It is hosted on a separate system that does not have dependencies in local host servers for access control, and it is optimized for files of all different sizes and uses.

**NEW QUESTION: 107**
Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?
**A.** Six months
**B.** One month
**C.** One year
**D.** One week
**Answer: A (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
SOC Type 2 reports are focused on the same policies and procedures, as well as their effectiveness, as SOC Type 1 reports, but are evaluated over a period of at least six consecutive months, rather than a finite point in time.

**NEW QUESTION: 108**
Cryptographic keys should be secured _____ .
**A.** To a level at least as high as the data they can decrypt
**B.** In vaults
**C.** With two-person integrity
**D.** By armed guards
**Answer: A (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
The physical security of crypto keys is of some concern, but guards or vaults are not always necessary.
Two-person integrity might be a good practice for protecting keys. The best answer to this question is option A, because it is always true, whereas the remaining options depend on circumstances.

**NEW QUESTION: 109**
All of the following are identity federation standards commonly found in use today except _____.
Response:
**A.** OpenID
**B.** OAuth
**C.** WS-Federation
**D.** PGP
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 110**

Every security program and process should have which of the following?
**A.** Severe penalties
**B.** Multifactor authentication
**C.** Foundational policy
**D.** Homomorphic encryption
**Answer: C (LEAVE A REPLY)**
Policy drives all programs and functions in the organization; the organization should not conduct any operations that don't have a policy governing them. Penalties may or may not be an element of policy, and severity depends on the topic. Multifactor authentication and homomorphic encryption are red herrings here.

**NEW QUESTION: 111**
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 (LEAVE A REPLY)**
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: 112**
Which of the following represents a minimum guaranteed resource within a cloud environment for the cloud customer?
**A.** Reservation
**B.** Share
**C.** Limit
**D.** Provision
**Answer: A (LEAVE A REPLY)**
A reservation is a minimum resource that is guaranteed to a customer within a cloud environment. Within a cloud, a reservation can pertain to the two main aspects of computing:
memory and processor. With a reservation in place, the cloud provider guarantees that a cloud customer will always have at minimum the necessary resources available to power on and operate any of their services.

**NEW QUESTION: 113**

Although host-based and network-based IDSs perform similar functions and have similar capabilities, which of the following is an advantage of a network-based IDS over a host-based IDS, assuming all capabilities are equal?

**A.** Segregated from host systems

**B.** Network access

**C.** Scalability

**D.** External to system patching

**Answer: A (LEAVE A REPLY)**

Explanation

A network-based IDS has the advantage of being segregated from host systems, and as such, it would not be open to compromise in the same manner a host-based system would be. Although a network-based IDS would be external to system patching, this is not the best answer here because it is a minor concern compared to segregation due to possible host compromise. Scalability is also not the best answer because, although a network-based IDS does remove processing from the host system, it is not a primary security concern.

Network access is not a consideration because both a host-based IDS and a network-based IDS would have access to network resources.

**NEW QUESTION: 114**

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 (LEAVE A REPLY)**

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: 115**

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 (LEAVE A REPLY)**

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: 116**

What is a cloud storage architecture that manages the data in a hierarchy of files?

**A.** File-based storage

**B.** Object-based storage

**C.** CDN

**D.** Database

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 117**

What's a potential problem when object storage versus volume storage is used within IaaS for application use and dependency?

**A.** Object storage is only optimized for small files.

**B.** Object storage is its own system, and data consistency depends on replication.

**C.** Object storage may have availability issues.

**D.** Object storage is dependent on access control from the host server.

**Answer: B (LEAVE A REPLY)**

Object storage runs on its own independent systems, which have their own redundancy and distribution. To ensure data consistency, sufficient time is needed for objects to fully replicate to all potential locations before being accessed. Object storage is optimized for high availability and will not be any less reliable than any other virtual machine within a cloud environment. It is hosted on a separate system that does not have dependencies in local host servers for access control, and it is optimized for files of all different sizes and uses.

**NEW QUESTION: 118**

A crucial decision any company must make is in regard to where it hosts the data systems it depends on. A debate exists as to whether it's best to lease space in a data center or build your own data center--and now with cloud computing, whether to purchase resources within a cloud.

What is the biggest advantage to leasing space in a data center versus procuring cloud services?

**A.** Regulations

**B.** Control

**C.** Security

**D.** Costs

**Answer: B (LEAVE A REPLY)**

When leasing space in a data center versus utilizing cloud services, a customer has a much greater control over its systems and services, from both the hardware/software perspective and the operational management perspective. Costs, regulations, and security are all prime considerations regardless of the hosting type selected. Although regulations will be the same in either hosting solution, in most instances, costs and security will be greater factors with leased space.

**NEW QUESTION: 119**

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 (LEAVE A REPLY)**

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: 120**

Where is an XML firewall most commonly deployed in the environment?

**A.** Between the application and data layers

**B.** Between the IPS and firewall

**C.** Between the presentation and application layers

**D.** Between the firewall and application server

**Answer: (SHOW ANSWER)**

Explanation

XML firewalls are most commonly deployed in line between the firewall and application server to validate XML code before it reaches the application.

**NEW QUESTION: 121**

Which of the following is a risk that stems from a virtualized environment?

Response:

**A.** It is difficult to find and contract with multiple utility providers of the same type (electric, water, etc.).
**B.** Modern SLA demands are stringent and very hard to meet.
**C.** Cloud data centers can become a single point of failure.
**D.** Live virtual machines in the production environment are moved from one host to another in the clear.
**Answer: D (LEAVE A REPLY)**



**NEW QUESTION: 122**
Your organization is developing software for wide use by the public. You have decided to test it in a cloud environment, in a PaaS model. Which of the following should be of particular concern to your organization for this situation?
Response:
**A.** Regulatory compliance
**B.** Vendor lock-in
**C.** Backdoors
**D.** High-speed network connectivity
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 123**
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: (SHOW ANSWER)**
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: 124**
Which of the following is considered an administrative control?
**A.** Keystroke logging
**B.** Access control process
**C.** Door locks
**D.** Biometric authentication
**Answer: B (LEAVE A REPLY)**
A process is an administrative control; sometimes, the process includes elements of other types of controls (in this case, the access control mechanism might be a technical control, or it might be a physical control), but the process itself is administrative. Keystroke logging is a technical control (or an attack, if done for malicious purposes, and not for auditing); door locks are a physical control; and biometric authentication is a technological control.

**NEW QUESTION: 125**
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 (LEAVE A REPLY)**
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: 126**
Every cloud service provider that opts to join the CSA STAR program registry must complete a _____.
**A.** Consensus Assessment Initiative Questionnaire (CAIQ)
**B.** SOC 2, Type 2 audit report
**C.** ISO 27001 ISMS review

**D.** NIST 800-37 RMF audit
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 127**
In application-level encryption, where does the encryption engine reside?
**A.** In the OS on which the application is run
**B.** In the volume where the database resides
**C.** Within the database accessed by the application
**D.** In the application accessing the database
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 128**
Which of the following data sanitation methods would be the MOST effective if you needed to securely remove data as quickly as possible in a cloud environment?
Response:
**A.** Degaussing
**B.** Cryptographic erasure
**C.** Overwriting
**D.** Zeroing
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 129**
Which protocol, as a part of TLS, handles the actual secure communications and transmission of data?
**A.** Negotiation
**B.** Handshake
**C.** Transfer
**D.** Record
**Answer: D (LEAVE A REPLY)**
Explanation
The TLS record protocol is the actual secure communications method for transmitting data; it's responsible for encrypting and authenticating packets throughout their transmission between the parties, and in some cases it also performs compression. The TLS handshake protocol is what negotiates and establishes the TLS connection between two parties and enables the secure communications channel to then handle data transmissions.
Negotiation and transfer are not protocols under TLS.

**NEW QUESTION: 130**
Other than cost savings realized due to measured service, what is another facet of cloud computing that will typically save substantial costs in time and money for an organization in the event of a disaster?

**A.** Broad network access
**B.** Interoperability
**C.** Resource pooling
**D.** Portability
**Answer: A (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
With a typical BCDR solution, an organization would need some number of staff to quickly travel to the location of the BCDR site to configure systems and applications for recovery. With a cloud environment, everything is done over broad network access, with no need (or even possibility) to travel to a remote site at any time.

**NEW QUESTION: 131**
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: (SHOW ANSWER)**
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: 132**
Which of the following roles involves overseeing billing, purchasing, and requesting audit reports for an organization within a cloud environment?
**A.** Cloud service user
**B.** Cloud service business manager
**C.** Cloud service administrator
**D.** Cloud service integrator
**Answer: B (LEAVE A REPLY)**
The cloud service business manager is responsible for overseeing business and billing administration, purchasing cloud services, and requesting audit reports when necessary

**NEW QUESTION: 133**

What is the intellectual property protection for the tangible expression of a creative idea?
**A.** Trade secret
**B.** Copyright
**C.** Trademark
**D.** Patent
**Answer: (SHOW ANSWER)**
Explanation
Copyrights are protected tangible expressions of creative works. The other answers listed are answers to subsequent questions.

**NEW QUESTION: 134**
Heating, ventilation, and air conditioning (HVAC) systems cool the data center by pushing warm air into _____.
**A.** The outside world
**B.** Underfloor plenums
**C.** HVAC intakes
**D.** The server inlets
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 135**
Which technology is NOT commonly used for security with data in transit?
**A.** DNSSEC
**B.** IPsec
**C.** VPN
**D.** HTTPS
**Answer: A (LEAVE A REPLY)**
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: 136**
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: (SHOW ANSWER)**
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: 137**
With software-defined networking, what aspect of networking is abstracted from the forwarding of traffic?
**A.** Routing
**B.** Session
**C.** Filtering
**D.** Firewalling
**Answer: (SHOW ANSWER)**
Explanation
With software-defined networking (SDN), the filtering of network traffic is separated from the forwarding of network traffic so that it can be independently administered.

**NEW QUESTION: 138**
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: (SHOW ANSWER)**
Explanation/Reference:
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: 139**
Which of the following is not a security concern related to archiving data for long-term storage?
Response:
**A.** Format of the data
**B.** Underground depth of the storage facility
**C.** Long-term storage of the related cryptographic keys
**D.** Media the data resides on
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 140**
A denial of service (DoS) attack can potentially impact all customers within a cloud environment with the continued allocation of additional resources. Which of the following can be useful for a customer to protect themselves from a DoS attack against another customer?
**A.** Shares
**B.** Reservations
**C.** Limits
**D.** Borrows
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 141**
Which of the following is not an example of a highly regulated environment?
**A.** Financial services
**B.** Healthcare
**C.** Public companies
**D.** Wholesale or distribution
**Answer: D (LEAVE A REPLY)**
Wholesalers or distributors are generally not regulated, although the products they sell may be.

**NEW QUESTION: 142**
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 (LEAVE A REPLY)**
Explanation/Reference:
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: 143**
Which of the following terms is NOT a commonly used category of risk acceptance?
**A.** Moderate
**B.** Critical
**C.** Minimal
**D.** Accepted
**Answer: D (LEAVE A REPLY)**
Explanation/Reference:
Explanation
Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

**NEW QUESTION: 144**
Penetration testing is a(n) _____ form of security assessment.
Response:
**A.** Inexpensive
**B.** Active
**C.** Comprehensive
**D.** Total
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 145**
Which of the following approaches would NOT be considered sufficient to meet the requirements of secure data destruction within a cloud environment?
**A.** Cryptographic erasure
**B.** Zeroing
**C.** Overwriting
**D.** Deletion

**Answer: D (LEAVE A REPLY)**
Explanation
Deletion merely removes the pointers to data on a system; it does nothing to actually remove and sanitize the data. As such, the data remains in a recoverable state, and more secure methods are needed to ensure it has been destroyed and is not recoverable by another party.

**NEW QUESTION: 146**
Which of the following in a federated environment is responsible for consuming authentication tokens?
**A.** Cloud services broker
**B.** Relying party
**C.** Identity provider
**D.** Authentication provider
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 147**
Having a reservation in a cloud environment can ensure operations continue in the event of high utilization across the cloud.
Which of the following would NOT be a capability covered by reservations?
**A.** Performing business operations
**B.** Starting virtual machines
**C.** Running applications
**D.** Auto-scaling
**Answer: D (LEAVE A REPLY)**
Explanation
A reservation will not guarantee auto-scaling is available because it involves the allocation of additional resources beyond what a cloud customer already has provisioned.
Reservations will guarantee minimal resources are available to start virtual machines, run applications, and perform normal business operations.

**NEW QUESTION: 148**
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 (LEAVE A REPLY)**
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: 149**
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 (LEAVE A REPLY)**
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: 150**
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: (SHOW ANSWER)**
Explanation/Reference:
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: 151**
What concept does the D represent within the STRIDE threat model?
**A.** Denial of service
**B.** Distributed
**C.** Data breach

**D.** Data loss

**Answer: A (LEAVE A REPLY)**

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



**NEW QUESTION: 152**

Which protocol does the REST API depend on?

**A.** HTTP

**B.** XML

**C.** SAML

**D.** SSH

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 153**

Which component of ITIL involves planning for the restoration of services after an unexpected outage or incident?

**A.** Continuity management

**B.** Problem management

**C.** Configuration management

**D.** Availability management

**Answer: A (LEAVE A REPLY)**

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. 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: 154**
Which of the following frameworks focuses specifically on design implementation and management?
**A.** ISO 31000:2009
**B.** ISO 27017
**C.** NIST 800-92
**D.** HIPAA
**Answer: A (LEAVE A REPLY)**
ISO 31000:2009 specifically focuses on design implementation and management. HIPAA refers to health care regulations, NIST 800-92 is about log management, and ISO 27017 is about cloud specific security controls.

**NEW QUESTION: 155**
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: (SHOW ANSWER)**
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: 156**
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 (LEAVE A REPLY)**
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: 157**
All of the following methods can be used to attenuate the harm caused by escalation of privilege except:
Response:
**A.** Periodic and effective use of cryptographic sanitization tools
**B.** Analysis and review of all log data by trained, skilled personnel on a frequent basis
**C.** The use of automated analysis tools such as SIM, SIEM, and SEM solutions
**D.** Extensive access control and authentication tools and techniques
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 158**
What are SOCI/SOCII/SOCIII?
Response:
**A.** Audit reports
**B.** Risk management frameworks
**C.** Access controls
**D.** Software development phases
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 159**
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 (LEAVE A REPLY)**
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: 160**
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
In order to increase the security value of the DLP, you should consider combining it with _____.

**A.** Digital rights management (DRM) and security event and incident management (SIEM) tools
**B.** Digital insurance policies
**C.** The Uptime Institute's Tier certification
**D.** An investment in upgraded project management software
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 161**
Data labels could include all the following, except:
Response:
**A.** Access restrictions
**B.** Confidentiality level
**C.** Distribution limitations
**D.** Multifactor authentication
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 162**
Which of the following is NOT a focus or consideration of an internal audit?
**A.** Certification
**B.** Design
**C.** Costs
**D.** Operational efficiency
**Answer: (SHOW ANSWER)**
In order to obtain and comply with certifications, independent external audits must be performed and satisfied.
Although some testing of certification controls can be part of an internal audit, they will not satisfy requirements.

**NEW QUESTION: 163**
The cloud deployment model that features joint ownership of assets among an affinity group is known as:
**A.** Hybrid
**B.** Public
**C.** Private
**D.** Community
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 164**
Which of the following threat types involves the sending of invalid and manipulated requests through a user's client to execute commands on the application under their own credentials?

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

**NEW QUESTION: 165**
Which of the following is NOT a major regulatory framework?
**A.** PCI DSS
**B.** HIPAA
**C.** SOX
**D.** FIPS 140-2
**Answer: D (LEAVE A REPLY)**
FIPS 140-2 is a United States certification standard for cryptographic modules, and it provides guidance and requirements for their use based on the requirements of the data classification. However, these are not actual regulatory requirements. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS) are all major regulatory frameworks either by law or specific to an industry.

**NEW QUESTION: 166**
Which of the following is NOT one of the main intended goals of a DLP solution?
**A.** Showing due diligence
**B.** Preventing malicious insiders
**C.** Regulatory compliance
**D.** Managing and minimizing risk
**Answer: B (LEAVE A REPLY)**

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



**NEW QUESTION: 167**
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 (LEAVE A REPLY)**
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: 168**
What are the U.S. State Department controls on technology exports known as?
**A.** DRM
**B.** ITAR
**C.** EAR
**D.** EAL
**Answer: B (LEAVE A REPLY)**

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

**NEW QUESTION: 169**
Which of the following may unilaterally deem a cloud hosting model inappropriate for a system or application?
**A.** Multitenancy
**B.** Certification
**C.** Regulation
**D.** Virtualization
**Answer: C (LEAVE A REPLY)**
Explanation
Some regulations may require specific security controls or certifications be used for hosting certain types of data or functions, and in some circumstances they may be requirements that are unable to be met by any cloud provider.

**NEW QUESTION: 170**
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 (LEAVE A REPLY)**
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: 171**
Which of the following is not a factor an organization might use in the cost-benefit analysis when deciding whether to migrate to a cloud environment?
**A.** Shifting from capital expenditures to support IT investment to operational expenditures
**B.** Branding associated with which cloud provider might be selected
**C.** The time savings and efficiencies offered by the cloud service
**D.** Pooled resources in the cloud
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 172**
On large distributed systems with pooled resources, cloud computing relies on extensive orchestration to maintain the environment and the constant provisioning of resources. Which of the following is crucial to the orchestration and automation of networking resources within a cloud?
**A.** DNSSEC
**B.** DNS
**C.** DCOM
**D.** DHCP
**Answer: D (LEAVE A REPLY)**
The Dynamic Host Configuration Protocol (DHCP) automatically configures network settings for a host so that these settings do not need to be configured on the host statically. Given the rapid and programmatic provisioning of resources within a cloud environment, this capability is crucial to cloud operations. Both DNS and its security-integrity extension DNSSEC provide name resolution to IP addresses, but neither is used for the configuration of network settings on a host. DCOM refers to the Distributed Component Object Model, which was developed by Microsoft as a means to request services across a network, and is not used for network configurations at all.

**NEW QUESTION: 173**
Data labels could include all the following, except:
**A.** Data value
**B.** Data of scheduled destruction
**C.** Date data was created
**D.** Data owner
**Answer: (SHOW ANSWER)**
All the others might be included in data labels, but we don't usually include data value, since it is prone to change frequently, and because it might not be information we want to disclose to anyone who does not have need to know.

**NEW QUESTION: 174**
What is a key component of GLBA?
**A.** The right to be forgotten
**B.** EU Data Directives
**C.** The information security program
**D.** The right to audit
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 175**
For optimal security, trust zones are used for network segmentation and isolation. They allow for the separation of various systems and tiers, each with its own security level.

Which of the following is typically used to allow administrative personnel access to trust zones?

**A.** IPSec

**B.** SSH

**C.** VPN

**D.** TLS

**Answer: (SHOW ANSWER)**

Explanation

Virtual private networks (VPNs) are used to provide administrative personnel with secure communication channels through security systems and into trust zones. They allow staff who perform system administration tasks to have access to ports and systems that are not allowed from the public Internet. IPSec is an encryption protocol for point-to-point communications at the network level, and may be used within a trust zone but not to give access into a trust zone. TLS enables encryption of communications between systems and services and would likely be used to secure the VPN communications, but it does not represent the overall concept being asked for in the question. SSH allows for secure shell access to systems, but not for general access into trust zones.

**NEW QUESTION: 176**

TLS provides and _____ for _____ communications.

Response:

**A.** Security, optimization

**B.** Privacy, integrity

**C.** Enhancement, privacy

**D.** Privacy, security

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 177**

You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment.

Management is interested in adopting an Agile development style.

This will be typified by which of the following traits?

**A.** Isolated programming experts for specific functional elements

**B.** Rigorous, repeated security testing

**C.** Reliance on a concrete plan formulated during the Define phase

**D.** Short, iterative work periods

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 178**

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: (SHOW ANSWER)**
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: 179**
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: (SHOW ANSWER)**
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: 180**
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "unvalidated redirects and forwards." Which of the following is a good way to protect against this problem?
Response:
**A.** Implement digital rights management (DRM) solutions.
**B.** Refrain from storing credentials long term.
**C.** Don't use redirects/forwards in your applications.
**D.** Implement security incident/event monitoring (security information and event management (SIEM)/security information management (SIM)/security event management (SEM)) solutions.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 181**
APIs are defined as which of the following?

**A.** A set of protocols, and tools for building software applications to access a web-based software application or tool
**B.** A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or tool
**C.** A set of standards for building software applications to access a web-based software application or tool
**D.** A set of routines and tools for building software applications to access web-based software applications
**Answer: B (LEAVE A REPLY)**
Explanation
All the answers are true, but B is the most complete.



**NEW QUESTION: 182**
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 (LEAVE A REPLY)**
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: 183**
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: (SHOW ANSWER)**
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: 184**
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 (LEAVE A REPLY)**
Explanation/Reference:
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: 185**

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: (SHOW ANSWER)**

Explanation/Reference:

Explanation:

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

**NEW QUESTION: 186**

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: (SHOW ANSWER)**

Explanation/Reference:

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: 187**

What is the only data format permitted with the SOAP API?

**A.** HTML

**B.** SAML

**C.** XSML

**D.** XML

**Answer: D (LEAVE A REPLY)**

Explanation/Reference:

Explanation:

The SOAP protocol only supports the XML data format.

**NEW QUESTION: 188**

Which of the following roles involves overseeing billing, purchasing, and requesting audit reports for an organization within a cloud environment?

**A.** Cloud service user
**B.** Cloud service business manager
**C.** Cloud service administrator
**D.** Cloud service integrator
**Answer: B (LEAVE A REPLY)**
Explanation
The cloud service business manager is responsible for overseeing business and billing administration, purchasing cloud services, and requesting audit reports when necessary

**NEW QUESTION: 189**
Which of the following cloud aspects complicates eDiscovery?
**A.** Resource pooling
**B.** On-demand self-service
**C.** Multitenancy
**D.** Measured service
**Answer: C (LEAVE A REPLY)**
Explanation
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: 190**
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 (LEAVE A REPLY)**
Explanation/Reference:
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: 191**
At which stage of the BCDR plan creation phase should security be included in discussions?
**A.** Define scope
**B.** Analyze
**C.** Assess risk
**D.** Gather requirements
**Answer: A (LEAVE A REPLY)**
Explanation
Explanation:
Security should be included in discussions from the very first phase when defining the scope. Adding security later is likely to incur additional costs in time and money, or will result in an incomplete or inadequate plan.

**NEW QUESTION: 192**
A data custodian is responsible for which of the following?
**A.** Data context
**B.** Data content
**C.** The safe custody, transport, storage of the data, and implementation of business rules
**D.** Logging access and alerts
**Answer: C (LEAVE A REPLY)**
A data custodian is responsible for the safe custody, transport, and storage of data, and the implementation of business roles.

**NEW QUESTION: 193**
What does dynamic application security testing (DAST) NOT entail?
**A.** Scanning
**B.** Probing
**C.** Discovery
**D.** Knowledge of the system
**Answer: D (LEAVE A REPLY)**
Explanation/Reference:
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: 194**
Which component of ITIL involves handling anything that can impact services for either internal or public users?

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

**NEW QUESTION: 195**
Although host-based and network-based IDSs perform similar functions and have similar capabilities, which of the following is an advantage of a network-based IDS over a host-based IDS, assuming all capabilities are equal?
**A.** Segregated from host systems
**B.** Network access
**C.** Scalability
**D.** External to system patching
**Answer: A (LEAVE A REPLY)**
A network-based IDS has the advantage of being segregated from host systems, and as such, it would not be open to compromise in the same manner a host-based system would be. Although a network-based IDS would be external to system patching, this is not the best answer here because it is a minor concern compared to segregation due to possible host compromise. Scalability is also not the best answer because, although a network-based IDS does remove processing from the host system, it is not a primary security concern.
Network access is not a consideration because both a host-based IDS and a network-based IDS would have access to network resources.

**NEW QUESTION: 196**
What changes are necessary to application code in order to implement DNSSEC?
**A.** Adding encryption modules
**B.** Implementing certificate validations
**C.** Additional DNS lookups
**D.** No changes are needed.
**Answer: D (LEAVE A REPLY)**

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



**NEW QUESTION: 197**
Aside from the fact that the cloud customer probably cannot locate/reach the physical storage assets of the cloud provider, and that wiping an entire storage space would impact other customers, why would degaussing probably not be an effective means of secure sanitization in the cloud?
**A.** Cloud data storage may not be affected by degaussing.
**B.** All the data storage space in the cloud is already gaussed.
**C.** Federal law prohibits it in the United States.
**D.** The blast radius is too wide.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 198**
Cloud environments pose many unique challenges for a data custodian to properly adhere to policies and the use of data. What poses the biggest challenge for a data custodian with a PaaS implementation, over and above the same concerns with IaaS?
Response:
**A.** Contractual requirements
**B.** Knowledge of systems
**C.** Access to systems
**D.** Data classification rules
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 199**
When using an Infrastructure as a Service solution, what is a key benefit provided to the customer?
**A.** The ability to scale up infrastructure services based on projected usage.
**B.** Increased energy and cooling system efficiencies.
**C.** Usage is metered and priced on the basis of units consumed.

**D.** Cost of ownership is transferred.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 200**
Which cloud storage type is typically used to house virtual machine images that are used throughout the environment?
**A.** Structured
**B.** Unstructured
**C.** Volume
**D.** Object
**Answer: D (LEAVE A REPLY)**
Explanation
Object storage is typically used to house virtual machine images because it is independent from other systems and is focused solely on storage. It is also the most appropriate for handling large individual files. Volume storage, because it is allocated to a specific host, would not be appropriate for the storing of virtual images.
Structured and unstructured are storage types specific to PaaS and would not be used for storing items used throughout a cloud environment.

**NEW QUESTION: 201**
Which of the following is NOT part of a retention policy?
**A.** Format
**B.** Costs
**C.** Accessibility
**D.** Duration
**Answer: B (LEAVE A REPLY)**
Explanation
Explanation:
The data retention policy covers the duration, format, technologies, protection, and accessibility of archives, but does not address the specific costs of its implementation and maintenance.

**NEW QUESTION: 202**
What is a key capability or characteristic of PaaS?
**A.** Support for a homogenous environment
**B.** Support for a single programming language
**C.** Ability to reduce lock-in
**D.** Ability to manually scale
**Answer: C (LEAVE A REPLY)**
PaaS should have the following key capabilities and characteristics:

- Support multiple languages and frameworks: PaaS should support multiple programming languages and frameworks, thus enabling the developers to code in whichever language they prefer or the design requirements specify. In recent times, significant strides and efforts have been taken to ensure that open source stacks are both supported and utilized, thus reducing "lock-in" or issues with interoperability when changing CSPs.
- Multiple hosting environments: The ability to support a wide variety of underlying hosting environments for the platform is key to meeting customer requirements and demands. Whether public cloud, private cloud, local hypervisor, or bare metal, supporting multiple hosting environments allows the application developer or administrator to migrate the application when and as required. This can also be used as a form of contingency and continuity and to ensure the ongoing availability.
- Flexibility: Traditionally, platform providers provided features and requirements that they felt suited the client requirements, along with what suited their service offering and positioned them as the provider of choice, with limited options for the customers to move easily. This has changed drastically, with extensibility and flexibility now afforded to meeting the needs and requirements of developer audiences. This has been heavily influenced by open source, which allows relevant plug-ins to be quickly and efficiently introduced into the platform.
- Allow choice and reduce lock-in: PaaS learns from previous horror stories and restrictions, proprietary meant red tape, barriers, and restrictions on what developers could do when it came to migration or adding features and components to the platform. Although the requirement to code to specific APIs was made available by the providers, they could run their apps in various environments based on commonality and standard API structures, ensuring a level of consistency and quality for customers and users.
- Ability to auto-scale: This enables the application to seamlessly scale up and down as required to accommodate the cyclical demands of users. The platform will allocate resources and assign these to the application as required. This serves as a key driver for any seasonal organizations that experience spikes and drops in usage.

**NEW QUESTION: 203**
Which of the following is not a way to manage risk?
Response:
**A.** Enveloping
**B.** Mitigating
**C.** Transferring
**D.** Accepting
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 204**
Which of the following is considered an administrative control?
**A.** Keystroke logging

**B.** Door locks
**C.** Biometric authentication
**D.** Access control process
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 205**
Which of the following aspects of the BC/DR process poses a risk to the organization?
Response:
**A.** Budgeting for disaster
**B.** Threat intelligence gathering
**C.** Full testing of the plan
**D.** Preplacement of response assets
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 206**
Which component of ITIL involves the creation of an RFC ticket and obtaining official approvals for it?
**A.** Problem management
**B.** Release management
**C.** Deployment management
**D.** Change management
**Answer: D (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
The change management process involves the creation of the official Request for Change (RFC) ticket, which is used to document the change, obtain the required approvals from management and stakeholders, and track the change to completion. Release management is a subcomponent of change management, where the actual code or configuration change is put into place. Deployment management is similar to release management, but it's where changes are actually implemented on systems. Problem management is focused on the identification and mitigation of known problems and deficiencies before they are able to occur.

**NEW QUESTION: 207**
When an organization is considering a cloud environment for hosting BCDR solutions, which of the following would be the greatest concern?
**A.** Self-service
**B.** Resource pooling
**C.** Availability
**D.** Location
**Answer: D (LEAVE A REPLY)**

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

**NEW QUESTION: 208**
Which concept BEST describes the capability for a cloud environment to automatically scale a system or application, based on its current resource demands?
**A.** On-demand self-service
**B.** Resource pooling
**C.** Measured service
**D.** Rapid elasticity
**Answer: D (LEAVE A REPLY)**
Explanation
Rapid elasticity allows a cloud environment to automatically add or remove resources to or from a system or application based on its current demands. Whereas a traditional data center model would require standby hardware and substantial effort to add resources in response to load increases, a cloud environment can easily and rapidly expand to meet resources demands, so long as the application is properly implemented for it.

**NEW QUESTION: 209**
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 (LEAVE A REPLY)**
The infrastructure service capability gives the cloud customer substantial control in provisioning and configuring resources, including processing, storage, and network resources.

**NEW QUESTION: 210**
Which of the following terms is NOT a commonly used category of risk acceptance?
**A.** Moderate
**B.** Critical
**C.** Minimal

**D.** Accepted
**Answer: D (LEAVE A REPLY)**
Explanation
Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

**NEW QUESTION: 211**
Which security concept is focused on the trustworthiness of data?
**A.** Integrity
**B.** Availability
**C.** Nonrepudiation
**D.** Confidentiality
**Answer: A (LEAVE A REPLY)**
Explanation
Integrity is focused on the trustworthiness of data as well as the prevention of unauthorized modification or tampering of it. A prime consideration for maintaining integrity is an emphasis on the change management and configuration management aspects of operations, so that all modifications are predictable, tracked, logged, and verified, whether they are performed by actual human users or systems processes and scripts.



**NEW QUESTION: 212**
A user signs on to a cloud-based social media platform. In another browser tab, the user finds an article worth posting to the social media platform. The user clicks on the platform's icon listed on the article's website, and the article is automatically posted to the user's account on the social media platform.
This is an example of what?
Response:
**A.** Insecure direct identifiers
**B.** Single sign-on
**C.** Identity federation
**D.** Cross-site scripting
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 213**
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: (SHOW ANSWER)**
Explanation/Reference:
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: 214**
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: (SHOW ANSWER)**
Explanation/Reference:
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: 215**
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 (LEAVE A REPLY)**
AES is an encryption standard. Link encryption is a method for protecting communications traffic. One-time pads are an encryption method.

**NEW QUESTION: 216**
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 (LEAVE A REPLY)**
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: 217**
Which of the following methods of addressing risk is most associated with insurance?
**A.** Mitigation
**B.** Transference
**C.** Avoidance
**D.** Acceptance
**Answer: B (LEAVE A REPLY)**
Explanation
Avoidance halts the business process, mitigation entails using controls to reduce risk, acceptance involves taking on the risk, and transference usually involves insurance.

**NEW QUESTION: 218**
Digital investigations have adopted many of the same methodologies and protocols as other types of criminal or scientific inquiries.

What term pertains to the application of scientific norms and protocols to digital investigations?

**A.** Scientific

**B.** Investigative

**C.** Methodological

**D.** Forensics

**Answer: D (LEAVE A REPLY)**

Explanation/Reference:

Explanation:

Forensics refers to the application of scientific methods and protocols to the investigation of crimes.

Although forensics has traditionally been applied to well-known criminal proceedings and investigations, the term equally applies to digital investigations and methods. Although the other answers provide similar- sounding terms and ideas, none is the appropriate answer in this case.

**NEW QUESTION: 219**

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: (SHOW ANSWER)**

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: 220**

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 (LEAVE A REPLY)**

Explanation/Reference:

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: 221**
Who is the entity identified by personal data?
**A.** The data processor
**B.** The data owner
**C.** The data custodian
**D.** The data subject
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 222**
What does dynamic application security testing (DAST) NOT entail?
**A.** Scanning
**B.** Probing
**C.** Discovery
**D.** Knowledge of the system
**Answer: (SHOW ANSWER)**
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: 223**
Legal controls refer to which of the following?
**A.** ISO 27001
**B.** PCI DSS
**C.** NIST 800-53r4
**D.** Controls designed to comply with laws and regulations related to the cloud environment
**Answer: (SHOW ANSWER)**
Explanation
Legal controls are those controls that are designed to comply with laws and regulations whether they be local or international.

**NEW QUESTION: 224**
Which term relates to the application of scientific methods and practices to evidence?
**A.** Forensics
**B.** Methodical
**C.** Theoretical
**D.** Measured
**Answer: A (LEAVE A REPLY)**

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

**NEW QUESTION: 225**
Which of the following is considered a technological control?
**A.** Firewall software
**B.** Firing personnel
**C.** Fireproof safe
**D.** Fire extinguisher
**Answer: A (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
A firewall is a technological control. The safe and extinguisher are physical controls and firing someone is an administrative control.

**NEW QUESTION: 226**
Although indirect identifiers cannot alone point to an individual, the more of them known can lead to a specific identity. Which strategy can be used to avoid such a connection being made?
Response:
**A.** Obfuscation
**B.** Anonymization
**C.** Encryption
**D.** Masking
**Answer: B (LEAVE A REPLY)**



**NEW QUESTION: 227**
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 (LEAVE A REPLY)**
Explanation/Reference:
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: 228**
What must SOAP rely on for security?
**A.** Encryption
**B.** Tokenization
**C.** TLS
**D.** SSL
**Answer: A (LEAVE A REPLY)**
Simple Object Access Protocol (SOAP) uses Extensible Markup Language (XML) for passing data, and it must rely on the encryption of those data packages for security.

**NEW QUESTION: 229**
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 (LEAVE A REPLY)**
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: 230**
Configurations and policies for a system can come from a variety of sources and take a variety of formats.
Which concept pertains to the application of a set of configurations and policies that is applied to all systems or a class of systems?
**A.** Hardening
**B.** Leveling
**C.** Baselines
**D.** Standards
**Answer: C (LEAVE A REPLY)**
Explanation
Baselines are a set of configurations and policies applied to all new systems or services, and they serve as the basis for deploying any other services on top of them. Although standards often form the basis for baselines, the term is applicable in this case. Hardening is the process of securing a system, often through the application of baselines. Leveling is an extraneous but similar term to baselining.

**NEW QUESTION: 231**
Without the extensive funds of a large corporation, a small-sized company could gain considerable and cost-effective services for which of the following concepts by moving to a cloud environment?
**A.** Regulatory
**B.** Security
**C.** Testing
**D.** Development
**Answer: B (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
Cloud environments, regardless of the specific deployment model used, have extensive and robust security controls in place, especially in regard to physical and infrastructure security. A small company can leverage the extensive security controls and monitoring provided by a cloud provider, which they would unlikely ever be able to afford on their own. Moving to a cloud would not result in any gains for development and testing because these areas require the same rigor regardless of where deployment and hosting occur.
Regulatory compliance in a cloud would not be a gain for an organization because it would likely result in additional oversight and auditing as well as require the organization to adapt to a new environment.

**NEW QUESTION: 232**
What are the U.S. Commerce Department controls on technology exports known as?

**A.** ITAR
**B.** DRM
**C.** EAR
**D.** EAL
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation:
EAR is a Commerce Department program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Digital rights management tools are used for protecting electronic processing of intellectual property.

**NEW QUESTION: 233**
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 (LEAVE A REPLY)**
Explanation
Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe. The rest are not.

**NEW QUESTION: 234**
Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?
**A.** Platform
**B.** Infrastructure
**C.** Governance
**D.** Application
**Answer: C (LEAVE A REPLY)**
Regardless of which cloud-hosting model is used, the cloud customer always has sole responsibility for the governance of systems and data.

**NEW QUESTION: 235**
The various models generally available for cloud BC/DR activities include all of the following except:
**A.** Private architecture, cloud backup
**B.** Cloud provider, backup from another cloud provider
**C.** Cloud provider, backup from same provider
**D.** Cloud provider, backup from private provider
**Answer: D (LEAVE A REPLY)**

This is not a normal configuration and would not likely provide genuine benefit.

**NEW QUESTION: 236**
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 (LEAVE A REPLY)**
Explanation/Reference:
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: 237**
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 (LEAVE A REPLY)**
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: 238**
Being in a cloud environment, cloud customers lose a lot of insight and knowledge as to how their data is stored and their systems are deployed.
Which concept from the ISO/IEC cloud standards relates to the necessity of the cloud provider to inform the cloud customer on these issues?
**A.** Disclosure
**B.** Transparency
**C.** Openness
**D.** Documentation
**Answer: (SHOW ANSWER)**

Transparency is the official process by which a cloud provider discloses insight and information into its configurations or operations to the appropriate audiences. Disclosure, openness, and documentation are all terms that sound similar to the correct answer, but none of them is the correct term in this case.

**NEW QUESTION: 239**
Which of the following is a risk associated with manual patching especially in the cloud?
Response:
**A.** Lack of applicability to the environment
**B.** No notice before the impact is realized
**C.** Patches may or may not address the vulnerability they were designed to fix.
**D.** The possibility for human error
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 240**
You are the security manager for a small application development company. Your company is considering the use of the cloud for software testing purposes. Which cloud service model is most likely to suit your needs?
**A.** IaaS
**B.** LaaS
**C.** SaaS
**D.** PaaS
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 241**
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 (LEAVE A REPLY)**
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: 242**
Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?
**A.** Six months
**B.** One month
**C.** One year
**D.** One week
**Answer: (SHOW ANSWER)**
SOC Type 2 reports are focused on the same policies and procedures, as well as their effectiveness, as SOC Type 1 reports, but are evaluated over a period of at least six consecutive months, rather than a finite point in time.

**NEW QUESTION: 243**
Which of the following is NOT a factor that is part of a firewall configuration?
**A.** Encryption
**B.** Port
**C.** Protocol
**D.** Source IP
**Answer: A (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
Firewalls take into account source IP, destination IP, the port the traffic is using, as well as the network protocol (UDP/TCP). Whether or not the traffic is encrypted is not something a firewall is concerned with.

**NEW QUESTION: 244**
What is the term that describes the situation when a malicious user/attacker can exit the restrictions of a single host and access other nodes on the network?
**A.** Escalation of privileges
**B.** Provider exit
**C.** Host escape
**D.** Guest escape

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 245**
How many additional DNS queries are needed when DNSSEC integrity checks are added?
**A.** Three
**B.** Zero
**C.** One
**D.** Two
**Answer: B (LEAVE A REPLY)**
DNSSEC does not require any additional DNS queries to be performed. The DNSSEC integrity checks and validations are all performed as part of the single DNS lookup resolution.

**NEW QUESTION: 246**
Which of the following threat types can occur when an application does not properly validate input and can be leveraged to send users to malicious sites that appear to be legitimate?
**A.** Unvalidated redirects and forwards
**B.** Insecure direct object references
**C.** Security miscomfiguration
**D.** Sensitive data exposure
**Answer: A (LEAVE A REPLY)**
Explanation
Many web applications offer redirect or forward pages that send users to different, external sites. If these pages are not properly secured and validated, attackers can use the application to forward users off to sites for phishing or malware attempts. These attempts can often be more successful than direct phishing attempts because users will trust the site or application that sent them there, and they will assume it has been properly validated and approved by the trusted application's owners or operators. 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. Sensitive data exposure occurs when an application does not use sufficient encryption and other security controls to protect sensitive application data.

**NEW QUESTION: 247**
Which Common Criteria Evaluation Assurance Level (EAL) is granted to those products that are formally verified in terms of design and tested by an independent third party?
**A.** 3
**B.** 1

**C.** 5
**D.** 7
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 248**
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: (SHOW ANSWER)**
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: 249**
What is the amount of fuel that should be on hand to power generators for backup datacenter power, in all tiers, according to the Uptime Institute?
**A.** 12 hours
**B.** 1,000 gallons
**C.** As much as needed to ensure all systems may be gracefully shut down and data securely stored
**D.** 1
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 250**
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 (LEAVE A REPLY)**
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: 251**
Which of the following is NOT one of the main intended goals of a DLP solution?
**A.** Showing due diligence

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

**NEW QUESTION: 252**
What concept does the "T" represent in the STRIDE threat model?
**A.** TLS
**B.** Testing
**C.** Tampering with data
**D.** Transport
**Answer: C (LEAVE A REPLY)**
Explanation/Reference:
Explanation
Any application that sends data to the user will face the potential that the user could manipulate or alter the data, whether it resides in cookies, GET or POST commands, or headers, or manipulates client-side validations. If the user receives data from the application, it is crucial that the application validate and verify any data that is received back from the user.

**NEW QUESTION: 253**
Your boss has tasked your team with getting your legacy systems and applications connected with new cloud-based services that management has decided are crucial to customer service and offerings.
Which role would you be assuming under this directive?
**A.** Cloud service administrator
**B.** Cloud service user
**C.** Cloud service integrator
**D.** Cloud service business manager
**Answer: C (LEAVE A REPLY)**
The cloud service integrator role is responsible for connecting and integrating existing services and applications with cloud-based services.A cloud service administrator is responsible for testing, monitoring, and securing cloud services, as well as providing usage

reporting and dealing with service problems. The cloud service user is someone who consumes cloud services. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

**NEW QUESTION: 254**
Which of these characteristics of a virtualized network adds risks to the cloud environment?
**A.** Self-service
**B.** Pay-per-use
**C.** Scalability
**D.** Redundancy
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 255**
The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet). In a typical TLS session, what is the usual means for establishing trust between the parties?
**A.** Multifactor authentication
**B.** PKI certificates
**C.** Out-of-band authentication
**D.** Preexisting knowledge of each other
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 256**
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 (LEAVE A REPLY)**
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: 257**
What is the intellectual property protection for a confidential recipe for muffins?
**A.** Patent
**B.** Trademark
**C.** Trade secret
**D.** Copyright
**Answer: C (LEAVE A REPLY)**
Confidential recipes unique to the organization are trade secrets. The other answers listed are answers to other questions.

**NEW QUESTION: 258**
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 (LEAVE A REPLY)**
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: 259**
Which security certification serves as a general framework that can be applied to any type of system or application?
Response:
**A.** PCI DSS
**B.** NIST SP 800-53

**C.** ISO/IEC 27001
**D.** FIPS 140-2
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 260**
What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?
**A.** Proxy
**B.** Bastion
**C.** Honeypot
**D.** WAF
**Answer: B (LEAVE A REPLY)**
Explanation/Reference:
Explanation:
A bastion host is a server that is fully exposed to the public Internet, but is extremely hardened to prevent attacks and is usually dedicated for a specific application or usage; it is not something that will serve multiple purposes. This singular focus allows for much more stringent security hardening and monitoring.

**NEW QUESTION: 261**
When designing a cloud data center, which of the following aspects is not necessary to ensure continuity of operations during contingency operations?
Response:
**A.** Extended battery backup
**B.** Broadband data connection
**C.** Physical access to the data center
**D.** Access to clean water
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 262**
Which type of testing uses the same strategies and toolsets that hackers would use?
**A.** Static
**B.** Malicious
**C.** Penetration
**D.** Dynamic
**Answer: (SHOW ANSWER)**
Explanation
Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discovery potential vulnerabilities. Although the term malicious captures much of the intent of penetration testing from the perspective of an attacker, it is not the best answer. Static and dynamic are two types of system testing--where static is

done offline and with knowledge of the system, and dynamic is done on a live system without any previous knowledge is associated--but neither describes the type of testing being asked for in the question.

**NEW QUESTION: 263**
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: (SHOW ANSWER)**
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: 264**
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 (LEAVE A REPLY)**
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: 265**
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 (LEAVE A REPLY)**
Explanation
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: 266**
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: (SHOW ANSWER)**
Explanation/Reference:
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: 267**
What is the best source for information about securing a physical asset's BIOS?
**A.** Security policies

**B.** Manual pages
**C.** Vendor documentation
**D.** Regulations
**Answer: C (LEAVE A REPLY)**
Explanation
Vendor documentation from the manufacturer of the physical hardware is the best source of best practices for securing the BIOS.