

# Exam Questions CCSP

Certified Cloud Security Professional

<https://www.2passeasy.com/dumps/CCSP/>



#### NEW QUESTION 1

- (Exam Topic 4)

Which of the following is considered a physical control?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 2

- (Exam Topic 4)

The cloud customer will have the most control of their data and systems, and the cloud provider will have the least amount of responsibility, in which cloud computing arrangement?

- A. IaaS
- B. SaaS
- C. Community cloud
- D. PaaS

**Answer:** A

#### Explanation:

IaaS entails the cloud customer installing and maintaining the OS, programs, and data; PaaS has the customer installing programs and data; in SaaS, the customer only uploads data. In a community cloud, data and device owners are distributed.

#### NEW QUESTION 3

- (Exam Topic 4)

Countermeasures for protecting cloud operations against external attackers include all of the following except:

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 4

- (Exam Topic 4)

What is the intellectual property protection for a confidential recipe for muffins?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 5

- (Exam Topic 4)

When data discovery is undertaken, three main approaches or strategies are commonly used to determine what the type of data, its format, and composition are for the purposes of classification.

Which of the following is NOT one of the three main approaches to data discovery?

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

**Answer:** B

#### Explanation:

Hashing involves taking a block of data and, through the use of a one-way operation, producing a fixed-size value that can be used for comparison with other data. It is used primarily for protecting data and allowing for rapid comparison when matching data values such as passwords. Labels involve looking for header

information or other categorizations of data to determine its type and possible classifications. Metadata involves looking at information attributes of the data, such as creator, application, type, and so on, in determining classification. Content analysis involves examining the actual data itself for its composition and classification level.

#### NEW QUESTION 6

- (Exam Topic 4)

Which of the following roles is responsible for creating cloud components and the testing and validation of services?

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 7

- (Exam Topic 4)

Which of the following concepts is NOT one of the core components to an encryption system architecture?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 8

- (Exam Topic 4)

What type of masking would you employ to produce a separate data set for testing purposes based on production data without any sensitive information?

- A. Dynamic
- B. Tokenized
- C. Replicated
- D. Static

**Answer:** D

#### Explanation:

Static masking involves taking a data set and replacing sensitive fields and values with non-sensitive or garbage data. This is done to enable testing of an application against data that resembles production data, both in size and format, but without containing anything sensitive. Dynamic masking involves the live and transactional masking of data while an application is using it. Tokenized would refer to tokenization, which is the replacing of sensitive data with a key value that can later be matched back to the original value, and although it could be used as part of the production of test data, it does not refer to the overall process. Replicated is provided as an erroneous answer, as replicated data would be identical in value and would not accomplish the production of a test set.

#### NEW QUESTION 9

- (Exam Topic 4)

Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 10

- (Exam Topic 4)

With the rapid emergence of cloud computing, very few regulations were in place that pertained to it specifically, and organizations often had to resort to using a collection of regulations that were not specific to cloud in order to drive audits and policies.

Which standard from the ISO/IEC was designed specifically for cloud computing?

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

**Answer:**

D

**Explanation:**

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

**NEW QUESTION 10**

- (Exam Topic 4)

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

**Explanation:**

A data custodian is responsible for the safe custody, transport, and storage of data, and the implementation of business roles.

**NEW QUESTION 11**

- (Exam Topic 4)

Countermeasures for protecting cloud operations against internal threats include all of the following except:

- A. Extensive and comprehensive training programs, including initial, recurring, and refresher sessions
- B. Skills and knowledge testing
- C. Hardened perimeter devices
- D. Aggressive background checks

**Answer:** C

**Explanation:**

Hardened perimeter devices are more useful at attenuating the risk of external attack.

**NEW QUESTION 16**

- (Exam Topic 4)

What are the U.S. State Department controls on technology exports known as?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 18**

- (Exam Topic 4)

Which kind of SSAE audit report is most beneficial for a cloud customer, even though it's unlikely the cloud provider will share it?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 20**

- (Exam Topic 4)

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

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

**Answer:** A

**Explanation:**

Cryptographic keys should not be stored along with the data they secure, regardless of key length. We don't split crypto keys or generate redundant keys (doing

so would violate the principle of secrecy necessary for keys to serve their purpose).

#### NEW QUESTION 24

- (Exam Topic 4)

Which of the following is NOT a component of access control?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 29

- (Exam Topic 4)

Cloud systems are increasingly used for BCDR solutions for organizations. What aspect of cloud computing makes their use for BCDR the most attractive?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 33

- (Exam Topic 4)

DLP solutions can aid in deterring loss due to which of the following?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 37

- (Exam Topic 4)

What is the intellectual property protection for the tangible expression of a creative idea?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 38

- (Exam Topic 4)

What is the experimental technology that might lead to the possibility of processing encrypted data without having to decrypt it first?

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

**Answer:**

C

**Explanation:**

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

**NEW QUESTION 42**

- (Exam Topic 4)

What type of solution is at the core of virtually all directory services?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 45**

- (Exam Topic 4)

What is an experimental technology that is intended to create the possibility of processing encrypted data without having to decrypt it first?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 46**

- (Exam Topic 4)

Which of the following best describes SAML?

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

**Answer:** D

**NEW QUESTION 48**

- (Exam Topic 4)

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

**Explanation:**

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 53**

- (Exam Topic 4)

Which component of ITIL involves handling anything that can impact services for either internal or public users?

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

**Answer:** A

**Explanation:**

Incident management is focused on limiting the impact of disruptions to an organization's services or operations, as well as returning their state to full operational status as soon as possible. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur. Deployment management is a subcomponent of change management and is where the actual code or configuration change is put into place. Change management involves the



processes and procedures that allow an organization to make changes to its IT systems and services in a controlled manner.

#### NEW QUESTION 56

- (Exam Topic 4)

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 obscure
- D. These are often used for authentication.
- E. Data masking involves stripping out all digits in a string of numbers so as to obscure the original number.

**Answer:** A

#### Explanation:

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 61

- (Exam Topic 4)

Which of the following technologies is NOT commonly used for accessing systems and services in a cloud environment in a secure manner?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 64

- (Exam Topic 4)

As a result of scandals involving publicly traded corporations such as Enron, WorldCom, and Adelphi, Congress passed legislation known as:

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 69

- (Exam Topic 4)

All the following are data analytics modes, except:

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 73

- (Exam Topic 4)

An audit scope statement defines the limits and outcomes from an audit.

Which of the following would NOT be included as part of an audit scope statement?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 76

- (Exam Topic 4)

Which of the following is a management role, versus a technical role, as it pertains to data management and oversight?

- A. Data owner
- B. Data processor
- C. Database administrator
- D. Data custodian

**Answer:** A

#### Explanation:

Data owner is a management role that's responsible for all aspects of how data is used and protected. The database administrator, data custodian, and data processor are all technical roles that involve the actual use and consumption of data, or the implementation of security controls and policies with the data.

#### NEW QUESTION 77

- (Exam Topic 4)

The different cloud service models have varying levels of responsibilities for functions and operations depending with the model's level of service.

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 81

- (Exam Topic 4)

Limits for resource utilization can be set at different levels within a cloud environment to ensure that no particular entity can consume a level of resources that impacts other cloud customers.

Which of the following is NOT a unit covered by limits?

- A. Hypervisor
- B. Cloud customer
- C. Virtual machine
- D. Service

**Answer:** A

#### Explanation:

The hypervisor level, as a backend cloud infrastructure component, is not a unit where limits may be applied to control resource utilization. Limits can be placed at the service, virtual machine, and cloud customer levels within a cloud environment.

#### NEW QUESTION 83

- (Exam Topic 4)

The cloud customer's trust in the cloud provider can be enhanced by all of the following except:

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 84

- (Exam Topic 4)

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



**Explanation:**

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 89**

- (Exam Topic 4)

IRM solutions allow an organization to place different restrictions on data usage than would otherwise be possible through traditional security controls.

Which of the following controls would be possible with IRM that would not with traditional security controls?

- A. Copy
- B. Read
- C. Delete
- D. Print

**Answer:** D

**Explanation:**

Traditional security controls would not be able to restrict a user from printing something that they have the ability to access and read, but IRM solutions would allow for such a restriction. If a user has permissions to read a file, he can also copy the file or print it under traditional controls, and the ability to modify or write will give the user the ability to delete.

**NEW QUESTION 93**

- (Exam Topic 4)

What does static application security testing (SAST) offer as a tool to the testers that makes it unique compared to other common security testing methodologies?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 95**

- (Exam Topic 4)

All of the following are terms used to describe the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 97**

- (Exam Topic 4)

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

**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 101**

- (Exam Topic 4)

What is the correct order of the phases of the data life cycle?

- A. Create, Use, Store, Share, Archive, Destroy
- B. Create, Archive, Store, Share, Use, Destroy

- C. Create, Store, Use, Archive, Share, Destroy
- D. Create, Store, Use, Share, Archive, Destroy

**Answer:** D

**Explanation:**

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

**NEW QUESTION 106**

- (Exam Topic 4)

Different security testing methodologies offer different strategies and approaches to testing systems, requiring security personnel to determine the best type to use for their specific circumstances.

What does dynamic application security testing (DAST) NOT entail that SAST does?

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

**Answer:** B

**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 it must be discovered during its testing. As with most types of testing, dynamic application security testing (DAST) involves probing, scanning, and a discovery process for system information.

**NEW QUESTION 109**

- (Exam Topic 4)

During the course of an audit, which of the following would NOT be an input into the control requirements used as part of a gap analysis.

- A. Contractual requirements
- B. Regulations
- C. Vendor recommendations
- D. Corporate policy

**Answer:** C

**Explanation:**

Vendor recommendations would not be pertinent to the gap analysis after an audit. Although vendor recommendations will typically play a role in the development of corporate policies or contractual requirements, they are not required. Regulations, corporate policy, and contractual requirements all determine the expected or mandated controls in place on a system.

**NEW QUESTION 113**

- (Exam Topic 4)

The GAPP framework was developed through a joint effort between the major Canadian and American professional accounting associations in order to assist their members with managing and preventing risks to the privacy of their data and customers.

Which of the following is the meaning of GAPP?

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

**Answer:** C

**NEW QUESTION 117**

- (Exam Topic 4)

Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 119**

- (Exam Topic 4)

When an organization is considering a cloud environment for hosting BCDR solutions, which of the following would be the greatest concern?

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

D. Location

**Answer:** D

**Explanation:**

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

**NEW QUESTION 121**

- (Exam Topic 4)

Data labels could include all the following, except:

- A. Multifactor authentication
- B. Access restrictions
- C. Confidentiality level
- D. Distribution limitations

**Answer:** A

**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 124**

- (Exam Topic 4)

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

**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 127**

- (Exam Topic 4)

The baseline should cover which of the following?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 130**

- (Exam Topic 4)

When crafting plans and policies for data archiving, we should consider all of the following, except:

- A. The backup process
- B. Immediacy of the technology
- C. Archive location
- D. The format of the data

**Answer:** D

**NEW QUESTION 134**

- (Exam Topic 4)

The goals of DLP solution implementation include all of the following, except:

- A. Elasticity
- B. Policy enforcement
- C. Data discovery

D. Loss of mitigation

**Answer:** A

**Explanation:**

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

**NEW QUESTION 135**

- (Exam Topic 4)

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

**Explanation:**

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 137**

- (Exam Topic 4)

Which of the following is NOT considered a type of data loss?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 138**

- (Exam Topic 4)

The goals of SIEM solution implementation include all of the following, except:

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 142**

- (Exam Topic 4)

Which of the following could be used as a second component of multifactor authentication if a user has an RSA token?

- A. Access card
- B. USB thumb drive
- C. Retina scan
- D. RFID

**Answer:** C

**Explanation:**

A retina scan could be used in conjunction with an RSA token because it is a biometric factor, and thus a different type of factor. An access card, RFID, and USB thumb drive are all items in possession of a user, the same as an RSA token, and as such would not be appropriate.

**NEW QUESTION 144**

- (Exam Topic 4)

DLP can be combined with what other security technology to enhance data controls?

- A. DRM
- B. Hypervisor
- C. SIEM
- D. Kerberos

**Answer:** A

**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 146**

- (Exam Topic 4)

Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 150**

- (Exam Topic 4)

What concept and operational process must be spelled out clearly, as far as roles and responsibilities go, between the cloud provider and cloud customer for the mitigation of any problems or security events?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 154**

- (Exam Topic 4)

When reviewing the BIA after a cloud migration, the organization should take into account new factors related to data breach impacts. One of these new factors is:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 159**

- (Exam Topic 4)

Identity and access management (IAM) is a security discipline that ensures which of the following?

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

**Answer:** B

**Explanation:**



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

#### NEW QUESTION 161

- (Exam Topic 4)

In a cloud environment, encryption should be used for all the following, except:

- A. Secure sessions/VPN
- B. Long-term storage of data
- C. Near-term storage of virtualized images
- D. Profile formatting

**Answer:** D

#### Explanation:

All of these activities should incorporate encryption, except for profile formatting, which is a made-up term.

#### NEW QUESTION 165

- (Exam Topic 4)

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:** A

#### 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 168

- (Exam Topic 4)

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

#### 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 169

- (Exam Topic 4)

The goals of SIEM solution implementation include all of the following, except:

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 174

- (Exam Topic 4)

Which ITIL component is focused on anticipating predictable problems and ensuring that configurations and operations are in place to prevent these problems from ever occurring?

- A. Availability management
- B. Continuity management



- C. Configuration management
- D. Problem management

**Answer:** D

**Explanation:**

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

**NEW QUESTION 179**

- (Exam Topic 4)

To protect data on user devices in a BYOD environment, the organization should consider requiring all the following, except:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 181**

- (Exam Topic 4)

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:** C

**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 182**

- (Exam Topic 4)

Many aspects of cloud computing bring enormous benefits over a traditional data center, but also introduce new challenges unique to cloud computing. Which of the following aspects of cloud computing makes appropriate data classification of high importance?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 183**

- (Exam Topic 4)

A main objective for an organization when utilizing cloud services is to avoid vendor lock-in so as to ensure flexibility and maintain independence. Which core concept of cloud computing is most related to vendor lock-in?

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

**Answer:** C

**Explanation:**

Portability is the ability for a cloud customer to easily move their systems, services, and applications among different cloud providers. By avoiding reliance on proprietary APIs and other vendor-specific cloud features, an organization can maintain flexibility to move among the various cloud providers with greater ease. Reversibility refers to the ability for a cloud customer to quickly and easy remove all their services and data from a cloud provider. Interoperability is the ability to

reuse services and components for other applications and uses. Scalability refers to the ability of a cloud environment to add or remove resources to meet current demands.

#### NEW QUESTION 187

- (Exam Topic 4)

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

#### 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 189

- (Exam Topic 4)

Which protocol operates at the network layer and provides for full point-to-point encryption of all communications and transmissions?

- A. IPSec
- B. VPN
- C. SSL
- D. TLS

**Answer:** A

#### Explanation:

IPSec is a protocol for encrypting and authenticating packets during transmission between two parties and can involve any type of device, application, or service. The protocol performs both the authentication and negotiation of security policies between the two parties at the start of the connection and then maintains these policies throughout the lifetime of the connection. TLS operates at the application layer, not the network layer, and is widely used to secure communications between two parties. SSL is similar to TLS but has been deprecated. Although a VPN allows a secure channel for communications into a private network from an outside location, it's not a protocol.

#### NEW QUESTION 190

- (Exam Topic 4)

Maintenance mode requires all of these actions except:

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 193

- (Exam Topic 4)

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

#### Explanation:

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

#### NEW QUESTION 195

- (Exam Topic 4)

Which protocol, as a part of TLS, handles the actual secure communications and transmission of data?

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 199

- (Exam Topic 4)

BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business. Which concept pertains to the amount of data and services needed to reach the predetermined level of operations?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 201

- (Exam Topic 4)

In the cloud motif, the data owner is usually:

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 202

- (Exam Topic 4)

Which of the following is not an example of a highly regulated environment?

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 205

- (Exam Topic 4)

Which component of ITIL pertains to planning, coordinating, executing, and validating changes and rollouts to production environments?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 210

- (Exam Topic 4)

Countermeasures for protecting cloud operations against internal threats include all of the following except:

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

**Answer:** D

**Explanation:**

Conflict of interest is a threat, not a control.

**NEW QUESTION 213**

- (Exam Topic 4)

SOC Type 1 reports are considered "restricted use," in that they are intended only for limited audiences and purposes. Which of the following is NOT a population that would be appropriate for a SOC Type 1 report?

- A. Current clients
- B. Auditors
- C. Potential clients
- D. The service organization

**Answer:** C

**Explanation:**

Potential clients are not served by SOC Type 1 audits. A Type 2 or Type 3 report would be appropriate for potential clients. SOC Type 1 reports are intended for restricted use, where only the service organization itself, current clients, or auditors would have access to them.

**NEW QUESTION 214**

- (Exam Topic 4)

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:** D

**Explanation:**

Legal controls are those controls that are designed to comply with laws and regulations whether they be local or international.

**NEW QUESTION 217**

- (Exam Topic 4)

What must SOAP rely on for security since it does not provide security as a built-in capability?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 219**

- (Exam Topic 4)

Which of the following is the least challenging with regard to eDiscovery in the cloud?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 220**

- (Exam Topic 4)

What is the concept of isolating an application from the underlying operating system for testing purposes?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 223**

- (Exam Topic 4)

Which of the following is a valid risk management metric?

- A. KPI
- B. KRI
- C. SOC
- D. SLA

**Answer:** B

**Explanation:**

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

**NEW QUESTION 227**

- (Exam Topic 4)

Which of the following types of data would fall under data rights management (DRM) rather than information rights management (IRM)?

- A. Personnel data
- B. Security profiles
- C. Publications
- D. Financial records

**Answer:** C

**Explanation:**

Whereas IRM is used to protect a broad range of data, DRM is focused specifically on the protection of consumer media, such as publications, music, movies, and so on. IRM is used to protect general institution data, so financial records, personnel data, and security profiles would all fall under the auspices of IRM.

**NEW QUESTION 229**

- (Exam Topic 4)

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

**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 234**

- (Exam Topic 4)

Your IT steering committee has, at a high level, approved your project to begin using cloud services. However, the committee is concerned with getting locked into a single cloud provider and has flagged the ability to easily move between cloud providers as a top priority. It also wants to save costs by reusing components.

Which cross-cutting aspect of cloud computing would be your primary focus as your project plan continues to develop and you begin to evaluate cloud providers?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 238**

- (Exam Topic 4)

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:** B

**Explanation:**

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**

- (Exam Topic 4)

Which of the following terms is NOT a commonly used category of risk acceptance?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 240**

- (Exam Topic 4)

Which of the following is the primary purpose of an SOC 3 report?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 242**

- (Exam Topic 4)

A comprehensive BCDR plan will encapsulate many or most of the traditional concerns of operating a system in any data center. However, what is one consideration that is often overlooked with the formulation of a BCDR plan?

- A. Availability of staff
- B. Capacity at the BCDR site
- C. Restoration of services
- D. Change management processes

**Answer:** C

**Explanation:**

BCDR planning tends to focus so much on the failing over of services in the case of a disaster that recovery back to primary hosting after the disaster is often overlooked. In many instances, this can be just as complex a process as failing over, if not more so. Availability of staff, capacity at the BCDR site, and change management processes are typically integral to BCDR plans and are common components of them.

**NEW QUESTION 243**

- (Exam Topic 4)

Tokenization requires two distinct \_\_\_\_\_.

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 248**

- (Exam Topic 3)

Which of the following aspects of security is solely the responsibility of the cloud provider?



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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 252**

- (Exam Topic 3)

The REST API is a widely used standard for communications of web-based services between clients and the servers hosting them. Which protocol does the REST API depend on?

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

**Answer:** A

**Explanation:**

Representational State Transfer (REST) is a software architectural scheme that applies the components, connectors, and data conduits for many web applications used on the Internet. It uses and relies on the HTTP protocol and supports a variety of data formats. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data. Secure Shell client (SSH) is a secure method for allowing remote login to systems over a network.

**NEW QUESTION 257**

- (Exam Topic 3)

You are working for a cloud service provider and receive an eDiscovery order pertaining to one of your customers. Which of the following would be the most appropriate action to take first?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 261**

- (Exam Topic 3)

With finite resources available within a cloud, even the largest cloud providers will at times need to determine which customers will receive additional resources first.

What is the term associated with this determination?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 263**

- (Exam Topic 3)

The president of your company has tasked you with implementing cloud services as the most efficient way of obtaining a robust disaster recovery configuration for your production services.

Which of the cloud deployment models would you MOST likely be exploring?

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

**Answer:** A

**Explanation:**

A hybrid cloud model spans two more different hosting configurations or cloud providers. This would enable an organization to continue using its current hosting configuration, while adding additional cloud services to enable disaster recovery capabilities. The other cloud deployment models--public, private, and community--would not be applicable for seeking a disaster recovery configuration where cloud services are to be leveraged for that purpose rather than production service hosting.

**NEW QUESTION 268**

- (Exam Topic 3)

Which cloud service category would be most ideal for a cloud customer that is developing software to test its applications among multiple hosting providers to determine the best option for its needs?

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

**Answer:** B

**Explanation:**

Platform as a Service would allow software developers to quickly and easily deploy their applications among different hosting providers for testing and validation in order to determine the best option. Although IaaS would also be appropriate for hosting applications, it would require too much configuration of application servers and libraries in order to test code. Conversely, PaaS would provide a ready-to-use environment from the onset. DaaS would not be appropriate in any way for software developers to use to deploy applications. IaaS would not be appropriate in this scenario because it would require the developers to also deploy and maintain the operating system images or to contract with another firm to do so. SaaS, being a fully functional software platform, would not be appropriate for deploying applications into.

**NEW QUESTION 273**

- (Exam Topic 3)

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:** D

**Explanation:**

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 278**

- (Exam Topic 3)

Jurisdictions have a broad range of privacy requirements pertaining to the handling of personal data and information.

Which jurisdiction requires all storage and processing of data that pertains to its citizens to be done on hardware that is physically located within its borders?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 282**

- (Exam Topic 3)

What does a cloud customer purchase or obtain from a cloud provider?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 285**

- (Exam Topic 3)

For service provisioning and support, what is the ideal amount of interaction between a cloud customer and cloud provider?

- A. Half
- B. Full
- C. Minimal
- D. Depends on the contract

**Answer:** C

**Explanation:**

The goal with any cloud-hosting setup is for the cloud customer to be able to perform most or all its functions for service provisioning and configuration without any need for support from or interaction with the cloud provider beyond the automated tools provided. To fulfill the tenants of on-demand self-service, required interaction with the cloud provider--either half time, full time, or a commensurate amount of time based on the contract--would be in opposition to a cloud's intended use. As such, these answers are incorrect.

**NEW QUESTION 290**

- (Exam Topic 3)

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

**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 293**

- (Exam Topic 3)

In order to prevent cloud customers from potentially consuming enormous amounts of resources within a cloud environment and thus having a negative impact on other customers, what concept is commonly used by a cloud provider?

- A. Limit
- B. Cap
- C. Throttle
- D. Reservation

**Answer:** A

**Explanation:**

A limit puts a maximum value on the amount of resources that may be consumed by either a system, a service, or a cloud customer. It is commonly used to prevent one entity from consuming enormous amounts of resources and having an operational impact on other tenants within the same cloud system. Limits can either be hard or somewhat flexible, meaning a customer can borrow from other customers while still having their actual limit preserved. A reservation is a guarantee to a cloud customer that a certain level of resources will always be available to them, regardless of what operational demands are currently placed on the cloud environment. Both cap and throttle are terms that sound similar to limit, but they are not the correct terms in this case.

**NEW QUESTION 296**

- (Exam Topic 3)

Within a federated identity system, which of the following would you be MOST likely to use for sending information for consumption by a relying party?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 298**

- (Exam Topic 3)

With software-defined networking (SDN), which two types of network operations are segregated to allow for granularity and delegation of administrative access and functions?

- A. Filtering and forwarding
- B. Filtering and firewalling
- C. Firewalling and forwarding

D. Forwarding and protocol

**Answer:** A

**Explanation:**

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

**NEW QUESTION 302**

- (Exam Topic 3)

Within a federated identity system, which entity accepts tokens from the identity provider?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 303**

- (Exam Topic 3)

DNSSEC was designed to add a layer of security to the DNS protocol. Which type of attack was the DNSSEC extension designed to mitigate?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 306**

- (Exam Topic 3)

Which of the following actions will NOT make data part of the create phase of the cloud data lifecycle?

- A. Modify data
- B. Modify metadata
- C. New data
- D. Import data

**Answer:** B

**Explanation:**

Modifying the metadata does not change the actual data. Although this initial phase is called "create," it can also refer to modification. In essence, any time data is considered "new," it is in the create phase. This can come from data that is newly created, data that is imported into a system and is new to that system, or data that is already present and is modified into a new form or value.

**NEW QUESTION 309**

- (Exam Topic 3)

Which cloud storage type requires special consideration on the part of the cloud customer to ensure they do not program themselves into a vendor lock-in situation?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 311**

- (Exam Topic 3)

Which of the following statements best describes a Type 1 hypervisor?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 316**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**NEW QUESTION 320**

- (Exam Topic 3)

Along with humidity, temperature is crucial to a data center for optimal operations and protection of equipment. Which of the following is the optimal temperature range as set by ASHRAE?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 322**

- (Exam Topic 3)

The share phase of the cloud data lifecycle involves allowing data to leave the application, to be shared with external systems, services, or even other vendors/contractors.

What technology would be useful for protecting data at this point?

- A. IDS
- B. DLP
- C. IPS
- D. WAF

**Answer:** B

**Explanation:**

Data loss prevention (DLP) solutions allow for control of data outside of the application or original system. They can enforce granular control such as printing, copying, and being read by others, as well as forcing expiration of access. Intrusion detection system (IDS) and intrusion prevention system (IPS) solutions are used for detecting and blocking suspicious and malicious traffic, respectively, whereas a web application firewall (WAF) is used for enforcing security or other controls on web-based applications.

**NEW QUESTION 325**

- (Exam Topic 3)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 328**

- (Exam Topic 3)

When dealing with PII, which category pertains to those requirements that can carry legal sanctions or penalties for failure to adequately safeguard the data and address compliance requirements?



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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 333**

- (Exam Topic 3)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 336**

- (Exam Topic 3)

Humidity levels for a data center are a prime concern for maintaining electrical and computing resources properly as well as ensuring that conditions are optimal for top performance.

Which of the following is the optimal humidity level, as established by ASHRAE?

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

**Answer:** C

**Explanation:**

The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) recommends 40 to 60 percent relative humidity for data centers. None of these options is the recommendation from ASHRAE.

**NEW QUESTION 338**

- (Exam Topic 3)

Different types of audits are intended for different audiences, such as internal, external, regulatory, and so on. Which of the following audits are considered "restricted use" versus being for a more broad audience?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 343**

- (Exam Topic 3)

Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.

Which of the following is NOT a regulatory system from the United States federal government?

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

**Answer:** D

**Explanation:**



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

#### NEW QUESTION 348

- (Exam Topic 3)

Which of the following is NOT one of the main intended goals of a DLP solution?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 350

- (Exam Topic 3)

You were recently hired as a project manager at a major university to implement cloud services for the academic and administrative systems. Because the load and demand for services at a university are very cyclical in nature, commensurate with the academic calendar, which of the following aspects of cloud computing would NOT be a primary benefit to you?

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

**Answer:** B

#### Explanation:

Broad network access to cloud services, although it is an integral aspect of cloud computing, would not being a specific benefit to an organization with cyclical business needs. The other options would allow for lower costs during periods of low usage as well as provide the ability to expand services quickly and easily when needed for peak periods. Measured service allows a cloud customer to only use the resources it needs at the time, and resource pooling allows a cloud customer to access resources as needed. On-demand self-service enables the cloud customer to change its provisioned resources on its own, without the need to interact with the staff from the cloud provider.

#### NEW QUESTION 351

- (Exam Topic 3)

Which of the following tasks within a SaaS environment would NOT be something the cloud customer would be responsible for?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 354

- (Exam Topic 3)

Different certifications and standards take different approaches to data center design and operations. Although many traditional approaches use a tiered methodology, which of the following utilizes a macro-level approach to data center design?

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

**Answer:** A

#### Explanation:

The Infinity Paradigm of the International Data Center Authority (IDCA) takes a macro-level approach to data center design. The IDCA does not use a specific, focused approach on specific components to achieve tier status. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers.

#### NEW QUESTION 359

- (Exam Topic 3)

Implementing baselines on systems would take an enormous amount of time and resources if the staff had to apply them to each server, and over time, it would be almost impossible to keep all the systems in sync on an ongoing basis.

Which of the following is NOT a package that can be used for implementing and maintaining baselines across an enterprise?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 360**

- (Exam Topic 3)

With an API, various features and optimizations are highly desirable to scalability, reliability, and security. What does the REST API support that the SOAP API does NOT support?

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

**Answer: B**

**Explanation:**

The Simple Object Access Protocol (SOAP) does not support caching, whereas the Representational State Transfer (REST) API does. The other options are all capabilities that are either not supported by SOAP or not supported by any API and must be provided by external features.

**NEW QUESTION 365**

- (Exam Topic 3)

Many tools and technologies are available for securing or monitoring data in transit within a data center, whether it is a traditional data center or a cloud.

Which of the following is NOT a technology for securing data in transit?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 366**

- (Exam Topic 3)

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**

**Explanation:**

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 370**

- (Exam Topic 3)

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

**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 375**

- (Exam Topic 3)

Which aspect of SaaS will alleviate much of the time and energy organizations spend on compliance (specifically baselines)?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 380**

- (Exam Topic 3)

Which phase of the cloud data lifecycle would be the MOST appropriate for the use of DLP technologies to protect the data?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 381**

- (Exam Topic 3)

Many aspects and features of cloud computing can make eDiscovery compliance more difficult or costly. Which aspect of cloud computing would be the MOST complicating factor?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 382**

- (Exam Topic 3)

If you are running an application that has strict legal requirements that the data cannot reside on systems that contain other applications or systems, which aspect of cloud computing would be prohibitive in this case?

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

**Answer:** A

**Explanation:**

Multitenancy is the aspect of cloud computing that involves having multiple customers and applications running within the same system and sharing the same resources. Although considerable mechanisms are in place to ensure isolation and separation, the data and applications are ultimately using shared resources.

Broad network access refers to the ability to access cloud services from any location or client. Portability refers to the ability to easily move cloud services between different cloud providers, whereas elasticity refers to the capabilities of a cloud environment to add or remove services, as needed, to meet current demand.

#### NEW QUESTION 385

- (Exam Topic 3)

Which phase of the cloud data lifecycle represents the first instance where security controls can be implemented?

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

**Answer:** C

#### Explanation:

The store phase occurs immediately after the create phase, and as data is committed to storage structures, the first opportunity for security controls to be implemented is realized. During the create phase, the data is not yet part of a system where security controls can be applied, and although the use and share phases also entail the application of security controls, they are not the first phase where the process occurs.

#### NEW QUESTION 386

- (Exam Topic 3)

Which of the following aspects of cloud computing would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 389

- (Exam Topic 3)

In order to ensure ongoing compliance with regulatory requirements, which phase of the cloud data lifecycle must be tested regularly?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 391

- (Exam Topic 2)

Which of the following is NOT a domain of the Cloud Controls Matrix (CCM)?

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 393

- (Exam Topic 2)

Which crucial aspect of cloud computing can be most threatened by insecure APIs?

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

**Answer:**

A

**Explanation:**

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

**NEW QUESTION 397**

- (Exam Topic 2)

What concept does the "I" represent with the STRIDE threat model?

- A. Integrity
- B. Information disclosure
- C. IT security
- D. Insider threat

**Answer: B**

**Explanation:**

Perhaps the biggest concern for any user is having their personal and sensitive information disclosed by an application. There are many aspects of an application to consider with security and protecting this information, and it is very difficult for any application to fully ensure security from start to finish. The obvious focus is on security within the application itself, as well as protecting and storing the data.

**NEW QUESTION 399**

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the oversight of processes and systems, as well as to ensuring their compliance with specific policies and regulations?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 401**

- (Exam Topic 2)

Which of the following is NOT a function performed by the handshake protocol of TLS?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 403**

- (Exam Topic 2)

Which aspect of cloud computing makes it very difficult to perform repeat audits over time to track changes and compliance?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 408**

- (Exam Topic 2)

Which type of audit report is considered a "restricted use" report for its intended audience?

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



**Answer:** C

**Explanation:**

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

**NEW QUESTION 413**

- (Exam Topic 2)

Which of the following is NOT a key area for performance monitoring as far as an SLA is concerned?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 416**

- (Exam Topic 2)

Which of the following does NOT fall under the "IT" aspect of quality of service (QoS)?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 421**

- (Exam Topic 2)

Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 425**

- (Exam Topic 2)

Which process serves to prove the identity and credentials of a user requesting access to an application or data?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 429**

- (Exam Topic 2)

Which security concept, if implemented correctly, will protect the data on a system, even if a malicious actor gains access to the actual system?

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

**Answer:** B

**Explanation:**



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

#### NEW QUESTION 432

- (Exam Topic 2)

Which value refers to the amount of time it takes to recover operations in a BCDR situation to meet management's objectives?

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 437

- (Exam Topic 2)

Which approach is typically the most efficient method to use for data discovery?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 440

- (Exam Topic 2)

Which of the cloud deployment models requires the cloud customer to be part of a specific group or organization in order to host cloud services within it?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 441

- (Exam Topic 2)

From a security perspective, which of the following is a major concern when evaluating possible BCDR solutions?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 446

- (Exam Topic 2)

Which audit type has been largely replaced by newer approaches since 2011?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 451

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the requirements placed on the cloud provider by the cloud customer for minimum performance standards and requirements that must be met?

- A. Regulatory requirements
- B. SLAs
- C. Auditability
- D. Governance

**Answer: B**

#### Explanation:

Whereas a contract spells out general terms and costs for services, the SLA is where the real meat of the business relationship and concrete requirements come into play. The SLA spells out in clear terms the minimum requirements for uptime, availability, processes, customer service and support, security controls and requirements, auditing and reporting, and potentially many other areas that define the business relationship and the success of it.

#### NEW QUESTION 455

- (Exam Topic 2)

With software-defined networking, what aspect of networking is abstracted from the forwarding of traffic?

- A. Routing
- B. Session
- C. Filtering
- D. Firewalling

**Answer: C**

#### 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 459

- (Exam Topic 2)

Which type of controls are the SOC Type 1 reports specifically focused on?

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 463

- (Exam Topic 2)

What is an often overlooked concept that is essential to protecting the confidentiality of data?

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 464

- (Exam Topic 2)

What type of masking strategy involves replacing data on a system while it passes between the data and application layers?

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 467

- (Exam Topic 2)

Which of the following service capabilities gives the cloud customer the most control over resources and configurations?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 469

- (Exam Topic 2)

Which of the following is the MOST important requirement and guidance for testing during an audit?

- A. Stakeholders
- B. Shareholders
- C. Management
- D. Regulations

**Answer:** D

#### Explanation:

During any audit, regulations are the most important factor and guidelines for what must be tested. Although the requirements from management, stakeholders, and shareholders are also important, regulations are not negotiable and pose the biggest risk to any organization for compliance failure.

#### NEW QUESTION 472

- (Exam Topic 2)

Over time, what is a primary concern for data archiving?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 474

- (Exam Topic 2)

Which aspect of cloud computing would make the use of a cloud the most attractive as a BCDR solution?

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 476

- (Exam Topic 2)

Which of the following would be a reason to undertake a BCDR test?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 478

- (Exam Topic 2)

How many additional DNS queries are needed when DNSSEC integrity checks are added?

- A. Three
- B. Zero
- C. One
- D. Two

**Answer: B**

**Explanation:**

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 479**

- (Exam Topic 2)

What process is used within a clustered system to provide high availability and load balancing?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 484**

- (Exam Topic 2)

Which attribute of data poses the biggest challenge for data discovery?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 486**

- (Exam Topic 2)

Which entity requires all collection and storing of data on their citizens to be done on hardware that resides within their borders?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 487**

- (Exam Topic 2)

What does static application security testing (SAST) offer as a tool to the testers?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 490**

- (Exam Topic 2)

Which data point that auditors always desire is very difficult to provide within a cloud environment?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 493**

- (Exam Topic 2)

Which of the cloud cross-cutting aspects relates to the ability to reuse or move components of an application or service?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 494**

- (Exam Topic 2)

Which if the following is NOT one of the three components of a federated identity system transaction?

- A. Relying party
- B. Identity provider
- C. User
- D. Proxy relay

**Answer:** D

**NEW QUESTION 497**

- (Exam Topic 2)

What concept does the "R" represent with the DREAD model?

- A. Reproducibility
- B. Repudiation
- C. Risk
- D. Residual

**Answer:** A

**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 impossible exploit, up to 10, which signifies something that anyone from a simple function call could exploit, such as a URL.

**NEW QUESTION 499**

- (Exam Topic 2)

Which of the following is NOT a focus or consideration of an internal audit?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 501**

- (Exam Topic 2)

Which security concept would business continuity and disaster recovery fall under?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 502**

- (Exam Topic 2)

Which of the following service capabilities gives the cloud customer the least amount of control over configurations and deployments?

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

**Answer:** C

**Explanation:**

The software service capability gives the cloud customer a fully established application, where only minimal user configuration options are allowed.

**NEW QUESTION 505**

- (Exam Topic 2)

Which aspect of cloud computing makes data classification even more vital than in a traditional data center?

- A. Interoperability
- B. Virtualization
- C. Multitenancy
- D. Portability

**Answer:** C

**Explanation:**

With multiple tenants within the same hosting environment, any failure to properly classify data may lead to potential exposure to other customers and applications within the same environment.

**NEW QUESTION 509**

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CCSP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CCSP Product From:

<https://www.2passeasy.com/dumps/CCSP/>

## Money Back Guarantee

### CCSP Practice Exam Features:

- \* CCSP Questions and Answers Updated Frequently
- \* CCSP Practice Questions Verified by Expert Senior Certified Staff
- \* CCSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CCSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year