ISC2

Exam Questions CCSP

Certified Cloud Security Professional

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 4)
All of the following are techniques to enhance the portability of cloud data, in order to minimize the potential of vendor lock-in except:

A. Ensure there are no physical limitations to moving
B. Use DRM and DLP solutions widely throughout the cloud operation
C. Ensure favorable contract terms to support portability
D. Avoid proprietary data formats

Answer: B

Explanation:
DRM and DLP are used for increased authentication/access control and egress monitoring, respectively, and would actually decrease portability instead of enhancing it.

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)
Which of the following storage types is most closely associated with a database-type storage implementation?

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

Answer: D

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

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

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

Answer: A

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

NEW QUESTION 5
- (Exam Topic 4)
Which of the following is the best example of a key component of regulated PII?

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

Answer: D

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

NEW QUESTION 6
- (Exam Topic 4)
In which cloud service model is the customer required to maintain the OS?

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

Answer: A

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

NEW QUESTION 7
- (Exam Topic 4)
Which cloud service category most commonly uses client-side key management systems?

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

Answer: A

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

NEW QUESTION 8
- (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 9
- (Exam Topic 4)
Which ITIL component is an ongoing, iterative process of tracking all deployed and configured resources that an organization uses and depends on, whether they are hosted in a traditional data center or a cloud?

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

Answer: D

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

NEW QUESTION 10
- (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 10
- (Exam Topic 4)
The most pragmatic option for data disposal in the cloud is which of the following?

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

Answer: A

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

NEW QUESTION 14
- (Exam Topic 4)
Which ITIL component focuses on ensuring that system resources, processes, and personnel are properly allocated to meet SLA requirements?

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

Answer: B

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

NEW QUESTION 15
- (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 18
- (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 22
- (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 27
- (Exam Topic 4)
Data labels could include all the following, except:

A. Data value
B. Data of scheduled destruction
C. Date data was created
D. Data owner

Answer: A

Explanation:
All the others might be included in data labels, but we don't usually include data value, since it is prone to change frequently, and because it might not be information we want to disclose to anyone who does not have need to know.

NEW QUESTION 28
- (Exam Topic 4)
Which of the following is not a way to manage risk?

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

Answer: D

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

NEW QUESTION 33
- (Exam Topic 4)
Tokenization requires two distinct _____.

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

Answer: D

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

NEW QUESTION 37
- (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 42
- (Exam Topic 4)
Which of the following best describes a cloud carrier?

A. The intermediary who provides connectivity and transport of cloud providers and cloud consumers
B. A person or entity responsible for making a cloud service available to consumers
C. The person or entity responsible for transporting data across the Internet
D. The person or entity responsible for keeping cloud services running for customers

Answer: A

Explanation:
A cloud carrier is the intermediary who provides connectivity and transport of cloud services between cloud providers and cloud customers.

NEW QUESTION 47
- (Exam Topic 4)
Which of the following best describes the Organizational Normative Framework (ONF)?

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

Answer: D

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

NEW QUESTION 48
- (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 50
- (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 52
- (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 57
- (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 61
- (Exam Topic 4)
What is the intellectual property protection for a useful manufacturing innovation?

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

Answer: C

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

NEW QUESTION 63
- (Exam Topic 4)
Gap analysis is performed for what reason?

A. To begin the benchmarking process
B. To assure proper accounting practices are being used
C. To provide assurances to cloud customers
D. To ensure all controls are in place and working properly

Answer: A

Explanation:
The primary purpose of the gap analysis is to begin the benchmarking process against risk and security standards and frameworks.

NEW QUESTION 67
- (Exam Topic 4)
Which of the following are attributes of cloud computing?

A. Minimal management effort and shared resources
B. High cost and unique resources
C. Rapid provisioning and slow release of resources
D. Limited access and service provider interaction

Answer: A

Explanation:
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NEW QUESTION 71
- (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 76
- (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 78
- (Exam Topic 4)
What is one of the reasons a baseline might be changed?

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

Answer: A

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

NEW QUESTION 82
- (Exam Topic 4)
Which of the following is NOT a major regulatory framework?

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

Answer: D

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

NEW QUESTION 86
- (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 90
- (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 91
- (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 96
- (Exam Topic 4)
Which of the following report is most aligned with financial control audits?

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

Answer: C

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

NEW QUESTION 99
- (Exam Topic 4)
For performance purposes, OS monitoring should include all of the following except:

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

Answer: D

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

NEW QUESTION 103
- (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 108
- (Exam Topic 4)
When using a PaaS solution, what is the capability provided to the customer?

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

H. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Answer: B

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

NEW QUESTION 112
- (Exam Topic 4)
Which of the following methods of addressing risk is most associated with insurance?

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

Answer: B

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

NEW QUESTION 115
- (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 119
- (Exam Topic 4)
What concept does the A represent within the DREAD model?

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

Answer: A

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

NEW QUESTION 120
- (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 123
- (Exam Topic 4)
What are SOC 1/SOC 2/SOC 3?

A. Audit reports

B. Risk management frameworks
C. Access controls
D. Software developments

Answer: A

Explanation:
An SOC 1 is a report on controls at a service organization that may be relevant to a user entity's internal control over financial reporting. An SOC 2 report is based on the existing SysTrust and WebTrust principles. The purpose of an SOC 2 report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, or privacy. An SOC 3 report is also based on the existing SysTrust and WebTrust principles, like a SOC 2 report. The difference is that the SOC 3 report does not detail the testing performed.

NEW QUESTION 127
- (Exam Topic 4)
Proper implementation of DLP solutions for successful function requires which of the following?

A. Physical access limitations
B. USB connectivity
C. Accurate data categorization
D. Physical presence

Answer: C

Explanation:
DLP tools need to be aware of which information to monitor and which requires categorization (usually done upon data creation, by the data owners). DLPs can be implemented with or without physical access or presence. USB connectivity has nothing to do with DLP solutions.

NEW QUESTION 129
- (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 130
- (Exam Topic 4)
Which of the following is NOT one of the components of multifactor authentication?

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

Answer: C

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

NEW QUESTION 134
- (Exam Topic 4)
DLP solutions can aid in deterring loss due to which of the following?

A. Power failure
B. Performance
C. Bad policy
D. Malicious disclosure

Answer: D

Explanation:
DLP tools can identify outbound traffic that violates the organization's policies. DLP will not protect against losses due to performance issues or power failures. The DLP solution must be configured according to the organization's policies, so bad policies will attenuate the effectiveness of DLP tools, not the other way around.

NEW QUESTION 135
- (Exam Topic 4)
Which of the following areas of responsibility would be shared between the cloud customer and cloud provider within the Software as a Service (SaaS) category?

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

Answer: C

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

NEW QUESTION 138
- (Exam Topic 4)
Gathering business requirements can aid the organization in determining all of this information about organizational assets, except:

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

Answer: D

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

NEW QUESTION 142
- (Exam Topic 4)
Which of the following terms is not associated with cloud forensics?

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

Answer: D

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

NEW QUESTION 147
- (Exam Topic 4)
Upon completing a risk analysis, a company has four different approaches to addressing risk. Which approach it takes will be based on costs, available options, and adherence to any regulatory requirements from independent audits.
Which of the following groupings correctly represents the four possible approaches?

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

Answer: A

Explanation:
The four possible approaches to risk are as follows: accept (do not patch and continue with the risk), avoid (implement solutions to prevent the risk from occurring), transfer (take out insurance), and mitigate (change configurations or patch to resolve the risk). Each of these answers contains at least one incorrect approach name.

NEW QUESTION 148
- (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 153
- (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 158
- (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 159
- (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 162
- (Exam Topic 4)
What category of PII data can carry potential fines or even criminal charges for its improper use or disclosure?

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

Answer: C

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

NEW QUESTION 165
- (Exam Topic 4)
With a federated identity system, what does the identity provider send information to after a successful authentication?

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

Answer: A

Explanation:

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

NEW QUESTION 169
- (Exam Topic 4)
Which of the following is considered a technological control?

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

Answer: A

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

NEW QUESTION 170
- (Exam Topic 4)
To address shared monitoring and testing responsibilities in a cloud configuration, the provider might offer all these to the cloud customer except:

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

Answer: C

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

NEW QUESTION 173
- (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 177
- (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 182
- (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 183
- (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 187
- (Exam Topic 4)
Which aspect of cloud computing serves as the biggest challenge to using DLP to protect data at rest?

A. Portability
B. Resource pooling
C. Interoperability
D. Reversibility

Answer: B

Explanation:
Resource pooling serves as the biggest challenge to using DLP solutions to protect data at rest because data is spread across large systems, which are also shared by many different clients. With the data always moving and being distributed, additional challenges for protection are created versus a physical and isolated storage system. Portability is the ability to easily move between different cloud providers, and interoperability is focused on the ability to reuse components or services. Reversibility pertains to the ability of a cloud customer to easily and completely remove their data and services from a cloud provider.

NEW QUESTION 191
- (Exam Topic 4)
Which of the following is considered an administrative control?

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

Answer: B

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

NEW QUESTION 194
- (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 198
- (Exam Topic 4)
In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?

A. HIPAA
B. The contract
C. Statutes
D. Security control matrix

Answer: B

Explanation:
The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable. The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

NEW QUESTION 202
- (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 204
- (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 208
- (Exam Topic 4)
When beginning an audit, both the system owner and the auditors must agree on various aspects of the final audit report.
Which of the following would NOT be something that is predefined as part of the audit agreement?

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

Answer: A

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

NEW QUESTION 209
- (Exam Topic 4)
When using a SaaS solution, what is the capability provided to the customer?

A. To use the provider's applications running on a cloud infrastructur
B. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interfac
C. The consumer does manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
D. To use the consumer's applications running on a cloud infrastructur
E. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interfac
F. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
G. To use the consumer's applications running on a cloud infrastructur
H. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interfac
I. The consumer does manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
J. To use the provider's applications running on a cloud infrastructur
K. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interfac
L. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual

application capabilities, with the possible exception of limited user-specific application configuration settings.

Answer: D

Explanation:
According to "The NIST Definition of Cloud Computing," in SaaS, "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

NEW QUESTION 212
- (Exam Topic 4)
Which of the following is NOT one of the official risk rating categories?

A. Critical
B. Low
C. Catastrophic
D. Minimal

Answer: C

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

NEW QUESTION 215
- (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 218
- (Exam Topic 3)
What is a serious complication an organization faces from the compliance perspective with international operations?

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

Answer: A

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

NEW QUESTION 220
- (Exam Topic 3)
Where is a DLP solution generally installed when utilized for monitoring data in transit?

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

Answer: A

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

NEW QUESTION 223

- (Exam Topic 3)
An SLA contains the official requirements for contract performance and satisfaction between the cloud provider and cloud customer. Which of the following would NOT be a component with measurable metrics and requirements as part of an SLA?

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

Answer: B

Explanation:
Dealing with users or user access would not be an appropriate item for inclusion in an SLA specifically. However, user access and user experience would be covered indirectly through other metrics. Memory, CPU, and network resources are all typically included within an SLA for availability and response times when dealing with any incidents.

NEW QUESTION 226
- (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 229
- (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 231
- (Exam Topic 3)
Where is an XML firewall most commonly and effectively deployed in the environment?

A. Between the application and data layers
B. Between the presentation and application layers
C. Between the IPS and firewall
D. Between the firewall and application server

Answer: D

Explanation:
An XML firewall is most commonly deployed in line between the firewall and application server to validate XML code before it reaches the application. An XML firewall is intended to validate XML before it reaches the application. Placing the XML firewall between the presentation and application layers, between the firewall and IPS, or between the application and data layers would not serve the intended purpose.

NEW QUESTION 235
- (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 240
- (Exam Topic 3)
Which cloud storage type is typically used to house virtual machine images that are used throughout the environment?

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

Answer: D

Explanation:
Object storage is typically used to house virtual machine images because it is independent from other systems and is focused solely on storage. It is also the most appropriate for handling large individual files. Volume storage, because it is allocated to a specific host, would not be appropriate for the storing of virtual images. Structured and unstructured are storage types specific to PaaS and would not be used for storing items used throughout a cloud environment.

NEW QUESTION 244
- (Exam Topic 3)
If a key feature of cloud computing that your organization desires is the ability to scale and expand without limit or concern about available resources, which cloud deployment model would you MOST likely be considering?

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

Answer: A

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

NEW QUESTION 247
- (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 250
- (Exam Topic 3)
Which data state would be most likely to use digital signatures as a security protection mechanism?

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

Answer: A

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

NEW QUESTION 254
- (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 258
- (Exam Topic 3)
If a company needed to guarantee through contract and SLAs that a cloud provider would always have available sufficient resources to start their services and provide a certain level of provisioning, what would the contract need to refer to?

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

Answer: B

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

NEW QUESTION 260
- (Exam Topic 3)
Many of the traditional concepts of systems and services for a traditional data center also apply to the cloud. Both are built around key computing concepts.
Which of the following compromise the two facets of computing?

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

Answer: C

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

NEW QUESTION 262
- (Exam Topic 3)
Most APIs will support a variety of different data formats or structures.
However, the SOAP API will only support which one of the following data formats?

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

Answer: A

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

NEW QUESTION 265
- (Exam Topic 3)
Which data state would be most likely to use TLS as a protection mechanism?

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

Answer: D

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

NEW QUESTION 266
- (Exam Topic 3)
From a security perspective, what component of a cloud computing infrastructure represents the biggest concern?

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

Answer: B

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

NEW QUESTION 267
- (Exam Topic 3)
There is a large gap between the privacy laws of the United States and those of the European Union. Bridging this gap is necessary for American companies to do business with European companies and in European markets in many situations, as the American companies are required to comply with the stricter requirements. Which US program was designed to help companies overcome these differences?

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

Answer: D

Explanation:
The Safe Harbor regulations were developed by the Department of Commerce and are meant to serve as a way to bridge the gap between privacy regulations of the European Union and the United States. Due to the lack of adequate privacy laws and protection on the federal level in the US, European privacy regulations generally prohibit the exporting of PII from Europe to the United States. Participation in the Safe Harbor program is voluntary on the part of US organizations. These organizations must conform to specific requirements and policies that mirror those from the EU, thus possibly fulfilling the EU requirements for data sharing and export. This way, American businesses can be allowed to serve customers in the EU. The Health Insurance Portability and Accountability Act (HIPAA) pertains to the protection of patient medical records and privacy. The Gramm-Leach-Bliley Act (GLBA) focuses on the use of PII within financial institutions. The Sarbanes-Oxley Act (SOX) regulates the financial and accounting practices used by organizations in order to protect shareholders from improper practices and errors.

NEW QUESTION 270
- (Exam Topic 3)
With IaaS, what is responsible for handling the security and control over the volume storage space?

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

Answer: B

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

NEW QUESTION 275
- (Exam Topic 3)
Firewalls are used to provide network security throughout an enterprise and to control what information can be accessed--and to a certain extent, through what means.
Which of the following is NOT something that firewalls are concerned with?

A. IP address
B. Encryption
C. Port
D. Protocol

Answer: B

Explanation:
Firewalls work at the network level and control traffic based on the source, destination, protocol, and ports. Whether or not the traffic is encrypted is not a factor with firewalls and their decisions about routing traffic. Firewalls work primarily with IP addresses, ports, and protocols.

NEW QUESTION 277
- (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 278
- (Exam Topic 3)
Within a SaaS environment, what is the responsibility on the part of the cloud customer in regard to procuring the software used?

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

Answer: B

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

NEW QUESTION 279
- (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 282
- (Exam Topic 3)
A crucial decision any company must make is in regard to where it hosts the data systems it depends on. A debate exists as to whether it's best to lease space in a data center or build your own data center--and now with cloud computing, whether to purchase resources within a cloud.
What is the biggest advantage to leasing space in a data center versus procuring cloud services?

A. Regulations
B. Control
C. Security
D. Costs

Answer: B

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

NEW QUESTION 285
- (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 288
- (Exam Topic 3)
You just hired an outside developer to modernize some applications with new web services and functionality. In order to implement a comprehensive test platform for validation, the developer needs a data set that resembles a production data set in both size and composition.
In order to accomplish this, what type of masking would you use?

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

Answer: C

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

NEW QUESTION 292
- (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 293
- (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 297
- (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 301
- (Exam Topic 3)
With a federated identity system, where would a user perform their authentication when requesting services or application access?

A. Cloud provider
B. The application

C. Their home organization
D. Third-party authentication system

Answer: C

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

NEW QUESTION 304
- (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 308
- (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 312
- (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 313
- (Exam Topic 2)
Which OSI layer does IPsec operate at?

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

Answer: A

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

NEW QUESTION 316
- (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 321
- (Exam Topic 2)
Which of the cloud deployment models involves spanning multiple cloud environments or a mix of cloud hosting models?

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

Answer: C

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

NEW QUESTION 326
- (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 329
- (Exam Topic 2)
What does the "SOC" acronym refer to with audit reports?

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

Answer: C

NEW QUESTION 334
- (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 339
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the requirements placed on a system or application by law, policy, or requirements from standards?

A. regulatory requirements
B. Auditability

C. Service-level agreements
D. Governance

Answer: A

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

NEW QUESTION 343
- (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 348
- (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 351
- (Exam Topic 2)
Which of the following is the sole responsibility of the cloud provider, regardless of which cloud model is used?

A. Platform
B. Data
C. Physical environment
D. Infrastructure

Answer: C

Explanation:
Regardless of which cloud-hosting model is used, the cloud provider always has sole responsibility for the physical environment.

NEW QUESTION 356
- (Exam Topic 2)
Which of the cloud deployment models offers the easiest initial setup and access for the cloud customer?

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

Answer: D

Explanation:
Because the public cloud model is available to everyone, in most instances all a customer will need to do to gain access is set up an account and provide a credit card number through the service's web portal. No additional contract negotiations, agreements, or specific group memberships are typically needed to get started.

NEW QUESTION 357
- (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 362
- (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 367
- (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 370
- (Exam Topic 2)
What process is used within a cloud environment to maintain resource balancing and ensure that resources are available where and when needed?

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

Answer: D

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

NEW QUESTION 372
- (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 374
- (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 376
- (Exam Topic 2)
Which of the following is NOT an application or utility to apply and enforce baselines on a system?

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

Answer: B

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

NEW QUESTION 381
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the assigning of jobs, tasks, and roles, as well as to ensuring they are successful and properly performed?

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

Answer: B

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

NEW QUESTION 382
- (Exam Topic 2)
Other than cost savings realized due to measured service, what is another facet of cloud computing that will typically save substantial costs in time and money for an organization in the event of a disaster?

A. Broad network access
B. Interoperability
C. Resource pooling
D. Portability

Answer: A

Explanation:
With a typical BCDR solution, an organization would need some number of staff to quickly travel to the location of the BCDR site to configure systems and applications for recovery. With a cloud environment, everything is done over broad network access, with no need (or even possibility) to travel to a remote site at any time.

NEW QUESTION 383
- (Exam Topic 2)
Which European Union directive pertains to personal data privacy and an individual's control over their personal data?

A. 99/9/EC
B. 95/46/EC
C. 2000/1/EC
D. 2013/27001/EC

Answer: B

Explanation:
Directive 95/46/EC is titled "On the protection of individuals with regard to the processing of personal data and on the free movement of such data."

NEW QUESTION 386
- (Exam Topic 2)
Which regulatory system pertains to the protection of healthcare data?

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

Answer: A

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

NEW QUESTION 388
- (Exam Topic 2)
Which of the cloud cross-cutting aspects relates to the ability to easily move services and applications between different cloud providers?

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

Answer: C

Explanation:
Portability is the ease with which a service or application can be moved between different cloud providers. Maintaining portability gives an organization great flexibility between cloud providers and the ability to shop for better deals or offerings.

NEW QUESTION 389
- (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 393
- (Exam Topic 2)
What type of security threat is DNSSEC designed to prevent?

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

Answer: C

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

NEW QUESTION 397
- (Exam Topic 2)
What type of data does data rights management (DRM) protect?

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

Answer: A

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

NEW QUESTION 400
- (Exam Topic 2)
The SOC Type 2 reports are divided into five principles.
Which of the five principles must also be included when auditing any of the other four principles?

A. Confidentiality
B. Privacy
C. Security
D. Availability

Answer: C

Explanation:
Under the SOC guidelines, when any of the four principles other than security are being audited, which includes availability, confidentiality, processing integrity, and privacy, the security principle must also be included with the audit.

NEW QUESTION 405
- (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 409
- (Exam Topic 2)
Which of the following should NOT be part of the requirement analysis phase of the software development lifecycle?

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

Answer: D

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

NEW QUESTION 414
- (Exam Topic 2)
Which of the following is NOT one of five principles of SOC Type 2 audits?

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

Answer: C

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

NEW QUESTION 415
- (Exam Topic 2)
Which of the following features is a main benefit of PaaS over IaaS?

A. Location independence
B. High-availability
C. Physical security requirements
D. Auto-scaling

Answer: D

Explanation:
With PaaS providing a fully configured and managed framework, auto-scaling can be implemented to programmatically adjust resources based on the current demands of the environment.

NEW QUESTION 416
- (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 420
- (Exam Topic 2)
Which of the following is NOT something that an HIDS will monitor?

A. Configurations
B. User logins
C. Critical system files
D. Network traffic

Answer: B

Explanation:
A host intrusion detection system (HIDS) monitors network traffic as well as critical system files and configurations.

NEW QUESTION 422
- (Exam Topic 2)
What does the REST API use to protect data transmissions?

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

Answer: D

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

NEW QUESTION 425
- (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 426
- (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 impossibly exploit, up to 10, which signifies something that anyone from a simple function call could exploit, such as a URL.

NEW QUESTION 430
- (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 432
- (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 433
- (Exam Topic 2)
Which type of testing uses the same strategies and toolsets that hackers would use?

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

Answer: A

Explanation:
Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discovery potential vulnerabilities.

NEW QUESTION 437
- (Exam Topic 2)
The European Union passed the first major regulation declaring data privacy to be a human right. In what year did it go into effect?

A. 2010
B. 2000
C. 1995
D. 1990

Answer: C

Explanation:
Adopted in 1995, Directive 95/46 EC establishes strong data protection and policy requirements, including the declaring of data privacy to be a human right. It establishes that an individual has the right to be notified when their personal data is being access or processed, that it only will ever be accessed for legitimate purposes, and that data will only be accessed to the exact extent it needs to be for the particular process or request.

NEW QUESTION 442
- (Exam Topic 1)
What does SDN stand for within a cloud environment?

A. Software-dynamic networking
B. Software-defined networking
C. Software-dependent networking
D. System-dynamic nodes

Answer: B

Explanation:
Software-defined networking separates the administration of network filtering and network forwarding to allow for distributed administration.

NEW QUESTION 443
- (Exam Topic 1)
Which of the following publishes the most commonly used standard for data center design in regard to tiers and topologies?

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

Answer: B

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

NEW QUESTION 445
- (Exam Topic 1)
Which of the following roles is responsible for creating cloud components and the testing and validation of services?

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

Answer: D

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

NEW QUESTION 447
- (Exam Topic 1)
Which of the following roles is responsible for peering with other cloud services and providers?

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

Answer: B

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

NEW QUESTION 450
- (Exam Topic 1)
What are the two protocols that TLS uses?

A. Handshake and record
B. Transport and initiate
C. Handshake and transport
D. Record and transmit

Answer: A

Explanation:
TLS uses the handshake protocol to establish and negotiate the TLS connection, and it uses the record protocol for the secure transmission of data.

NEW QUESTION 451
- (Exam Topic 1)
When is a virtual machine susceptible to attacks while a physical server in the same state would not be?

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

Answer: D

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

NEW QUESTION 455
- (Exam Topic 1)
From a legal perspective, what is the most important first step after an eDiscovery order has been received by the cloud provider?

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

Answer: A

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

NEW QUESTION 456
- (Exam Topic 1)
Within an Infrastructure as a Service model, which of the following would NOT be a measured service?

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

Answer: C

Explanation:
Within IaaS, the number of users on a system is not relevant to the particular hosting model in regard to cloud resources. IaaS is focused on infrastructure needs of a system or application. Therefore, a factor such as the number of users that could affect licensing requirements, for example, would apply to the SaaS model,

or in some instances to PaaS.

NEW QUESTION 459
- (Exam Topic 1)
Which protocol allows a system to use block-level storage as if it was a SAN, but over TCP network traffic instead?

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

Answer: B

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

NEW QUESTION 460
- (Exam Topic 1)
Which type of audit report does many cloud providers use to instill confidence in their policies, practices, and procedures to current and potential customers?

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

Answer: B

Explanation:
One approach that many cloud providers opt to take is to undergo a SOC 2 audit and make the report available to cloud customers and potential cloud customers as a way of providing security confidence without having to open their systems or sensitive information to the masses.

NEW QUESTION 465
- (Exam Topic 1)
Which of the following storage types is most closely associated with a database-type storage implementation?

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

Answer: D

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

NEW QUESTION 466
- (Exam Topic 1)
Which of the following is the optimal humidity level for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?

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

Answer: D

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

NEW QUESTION 468
- (Exam Topic 1)
If you're using iSCSI in a cloud environment, what must come from an external protocol or application?

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

Answer: D

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

NEW QUESTION 471

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

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

Answer: A

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

NEW QUESTION 473
- (Exam Topic 1)
What type of PII is regulated based on the type of application or per the conditions of the specific hosting agreement?

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

Answer: B

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

NEW QUESTION 477
- (Exam Topic 1)
Which of the following represents a control on the maximum amount of resources that a single customer, virtual machine, or application can consume within a cloud environment?

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

Answer: D

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

NEW QUESTION 480
- (Exam Topic 1)
Which of the following roles is responsible for preparing systems for the cloud, administering and monitoring services, and managing inventory and assets?

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

Answer: C

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

NEW QUESTION 482
- (Exam Topic 1)
Which of the following standards primarily pertains to cabling designs and setups in a data center?

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

Answer: B

Explanation:
The standards put out by Building Industry Consulting Service International (BICSI) primarily cover complex cabling designs and setups for data centers, but also include specifications on power, energy efficiency, and hot/cold aisle setups.

NEW QUESTION 483

- (Exam Topic 1)
Why does a Type 1 hypervisor typically offer tighter security controls than a Type 2 hypervisor?

A. A Type 1 hypervisor also controls patching of its hosted virtual machines ensure they are always secure.
B. A Type 1 hypervisor is tied directly to the bare metal and only runs with code necessary to perform its specific mission.
C. A Type 1 hypervisor performs hardware-level encryption for tighter security and efficiency.
D. A Type 1 hypervisor only hosts virtual machines with the same operating systems as the hypervisor.

Answer: B

Explanation:
Type 1 hypervisors run directly on top of the bare metal and only contain the code and functions required to perform their purpose. They do not rely on any other systems or contain extra features to secure.

NEW QUESTION 484
- (Exam Topic 1)
Which of the following approaches would NOT be considered sufficient to meet the requirements of secure data destruction within a cloud environment?

A. Cryptographic erasure
B. Zeroing
C. Overwriting
D. Deletion

Answer: D

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

NEW QUESTION 485
- (Exam Topic 1)
Which technology is NOT commonly used for security with data in transit?

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

Answer: A

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

NEW QUESTION 489
- (Exam Topic 1)
Which of the following is not a component of contractual PII?

A. Scope of processing
B. Value of data
C. Location of data
D. Use of subcontractors

Answer: C

Explanation:
The value of data itself has nothing to do with it being considered a part of contractual

NEW QUESTION 490
- (Exam Topic 1)
Which of the following pertains to fire safety standards within a data center, specifically with their enormous electrical consumption?

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

Answer: A

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

NEW QUESTION 495
- (Exam Topic 1)
What does the management plane typically utilize to perform administrative functions on the hypervisors that it has access to?

A. Scripts
B. RDP
C. APIs
D. XML

Answer: C

Explanation:
The functions of the management plane are typically exposed as a series of remote calls and function executions and as a set of APIs. These APIs are typically leveraged through either a client or a web portal, with the latter being the most common.

NEW QUESTION 496
- (Exam Topic 1)
Which of the following represents a minimum guaranteed resource within a cloud environment for the cloud customer?

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

Answer: A

Explanation:
A reservation is a minimum resource that is guaranteed to a customer within a cloud environment. Within a cloud, a reservation can pertain to the two main aspects of computing: memory and processor. With a reservation in place, the cloud provider guarantees that a cloud customer will always have at minimum the necessary resources available to power on and operate any of their services.

NEW QUESTION 500
- (Exam Topic 1)
Which of the following does NOT relate to the hiding of sensitive data from data sets?

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

Answer: B

Explanation:
Federation pertains to authenticating systems between different organizations.

NEW QUESTION 501
- (Exam Topic 1)
What type of masking strategy involves making a separate and distinct copy of data with masking in place?

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

Answer: C

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

NEW QUESTION 506
- (Exam Topic 1)
Which of the following roles is responsible for overseeing customer relationships and the processing of financial transactions?

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

Answer: C

Explanation:
The cloud service business manager is responsible for overseeing business plans and customer relationships as well as processing financial transactions.

NEW QUESTION 509
- (Exam Topic 1)
What is the primary reason that makes resolving jurisdictional conflicts complicated?

A. Different technology standards
B. Costs
C. Language barriers

D. Lack of international authority

Answer: D

Explanation:
With international operations, systems ultimately cross many jurisdictional boundaries, and many times, they conflict with each other. The major hurdle to overcome for an organization is the lack of an ultimate international authority to mediate such conflicts, with a likely result of legal efforts in each jurisdiction.

NEW QUESTION 510
- (Exam Topic 1)
Which technique involves replacing values within a specific data field to protect sensitive data?

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

Answer: B

Explanation:
Masking involves replacing specific data within a data set with new values. For example, with credit card fields, as most who have ever purchased anything online can attest, nearly the entire credit card number is masked with a character such as an asterisk, with the last four digits left visible for identification and confirmation.

NEW QUESTION 513
- (Exam Topic 1)
Which of the following roles involves overseeing billing, purchasing, and requesting audit reports for an organization within a cloud environment?

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

Answer: B

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

NEW QUESTION 517
- (Exam Topic 1)
What is the only data format permitted with the SOAP API?

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

Answer: D

Explanation:
The SOAP protocol only supports the XML data format.

NEW QUESTION 519
- (Exam Topic 1)
Which of the following is considered an internal redundancy for a data center?

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

Answer: A

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

NEW QUESTION 521
- (Exam Topic 1)
Which protocol does the REST API depend on?

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

Answer: A

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

NEW QUESTION 523
- (Exam Topic 1)
Why does a Type 2 hypervisor typically offer less security control than a Type 1 hypervisor?

A. A Type 2 hypervisor runs on top of another operating system and is dependent on the security of the OS for its own security.
B. A Type 2 hypervisor allows users to directly perform some functions with their own access.
C. A Type 2 hypervisor is open source, so attackers can more easily find exploitable vulnerabilities with that access.
D. A Type 2 hypervisor is always exposed to the public Internet for federated identity access.

Answer: A

Explanation:
A Type 2 hypervisor differs from a Type 1 hypervisor in that it runs on top of another operating system rather than directly tied into the underlying hardware of the virtual host servers. With this type of implementation, additional security and architecture concerns come into play because the interaction between the operating system and the hypervisor becomes a critical link. The hypervisor no longer has direct interaction and control over the underlying hardware, which means that some performance will be lost due to the operating system in the middle needing its own resources, patching requirements, and operational oversight.

NEW QUESTION 526
- (Exam Topic 1)
What is the best approach for dealing with services or utilities that are installed on a system but not needed to perform their desired function?

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

Answer: A

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

NEW QUESTION 529
- (Exam Topic 1)
Which of the following is considered an external redundancy for a data center?

A. Power feeds to rack
B. Generators
C. Power distribution units
D. Storage systems

Answer: B

Explanation:
Generators are considered an external redundancy to a data center. Power distribution units (PDUs), storage systems, and power feeds to racks are all internal to a data center, and as such they are considered internal redundancies.

NEW QUESTION 534
- (Exam Topic 1)
Which of the following are the storage types associated with IaaS?

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

Answer: A

NEW QUESTION 535
- (Exam Topic 1)
Which of the following threat types involves an application that does not validate authorization for portions of itself after the initial checks?

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

Answer: B

Explanation:
It is imperative that an application perform checks when each function or portion of the application is accessed, to ensure that the user is properly authorized to access it. Without continual checks each time a function is accessed, an attacker could forge requests to access portions of the application where authorization

has not been granted.

NEW QUESTION 536
......

Relate Links

100% Pass Your CCSP Exam with Exambible Prep Materials

https://www.exambible.com/CCSP-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/