Practice Exam Questions

(ISC)²

Certified Cloud Security Professional

EXAMKILLER

Help Pass Your Exam At First Try

Total Question: 450 QAs

Question No: 1
Breaking up information and storing encrypted information across different cloud storage solutions is known as:
A. Data dispersion
B. Bit Splitting
C. Tokenization
D. Bit Distribution
Answer: B
Explanation: This is the definition of Bit Splitting

Question No: 2
Which of the following can be deterred through implementation of Data Loss Prevention?
A. Seizure
B. Malicious Disclosure
C. Duplication
D. Encryption
Answer: B
Explanation: It helps in protecting data from malicious disclosure.
Data Loss Prevention. DLP. also known as data leakage prevention or data loss protection. Describes the controls put in place by an organization to ensure that certain types of data (structured and unstructured) remain under organizational controls. Inline with policies, standards, and procedures.

Question No: 3
Operating System management is done by customer in which service model of cloud computing?
A. IaaS
B. PaaS
C. SaaS
D. XaaS
Answer: A
Explanation: In IaaS model, operating system is managed by the customer.

Question No: 4
Which one of the following is used for da-ta-analytics?
A. Data Dispersion
B. Datamining
C. Data Allocation
D. Data sequencing
Answer: B
Explanation: Datamining:
When the organization has collected various data streams and can run queries across these various feeds, the organization can detect and analyze previously unknown trends and patterns that can be extremely useful.

--- Malisow, Ben. CCSP(ISC)2 Certified Cloud Security Professional Official Study Guide (Kindle Locations1960-1961). Wiley. Kindle Edition.

Question No: 5
Who is ultimately liable for all data loss and breaches in the cloud environment?
A. Cloud reseller
B. Cloud service provider
C. Cloud customer
D. Cloud access security broker(CASB)
Answer: C
Explanation: It is the customer who is ultimately responsible for any type of data loss or breaches.

Question No: 6
Security Governance, Risk and Compliance (GRC) is, generally, responsibility of which of the following across all the platforms (IaaS, PaaS and SaaS)?
A. Customer
B. Cloud Service Provider
C. Shared responsibility
D. Joint Responsibility
Answer: A
Explanation: GRC is responsibility of the customer across all service models.

Question No: 7
A framework to enable to cooperation between cloud consumers and cloud providers on demonstrating adequate risk management is:
A. ISO 31000
B. ISO 27005
C. CSA Cloud Control Matrix (CCM)
D. NIST 800-145
Answer: C
Explanation
CSA CCM is an inventory of cloud service security controls that are arranged into a hierarchy of security domains and enable to cooperation between cloud consumers and cloud providers on demonstrating adequate risk management.

Question No: 8
In Platform as a Service (PaaS). platform security is a responsibility of:
A. Customer
B. Cloud service provider
C. It's a shared responsibility
D. Neither of them
Answer: C
Explanation: This is a very confusing question and we need to understand that its a shared responsibility between cloud service provider and customer.

Question No: 9
When workstations can communicate with each other as though they were on a single, Dedicated LAN, it is known as:
A. DLAN
B. Dedicated LAN
C. LAN Binding
D. VLA
Answer: D
Explanation: The VM network requires as much protection as the physical one. Using VLANs can improve networking security in your environment. In simple terms, a VLAN is a set of workstations within a LAN that can communicate with each other as though they were on a single, isolated LAN. They are an Institute of Electrical and Electronics Engineers(IEEE) standard networking scheme with specific tagging methods that allow routing of packets to only those ports that are part of the VLAN.
--- Gordon, Adam. The Official (ISC)2 Guide to the CCSP CBK (Kindle Locations6557-6560). Wiley. Kindle Edition.

Question No: 10
Which of the following is key component of regulated PII components?
A. Mandatory Breach Reporting
B. Cloud Service Provider Consent
C. E-discovery
D. Data disclosure
Answer: A
Explanation: The key component and differentiator related to regulated PII is mandatory breach reporting requirements. At present, 47 states and territories within the United States, including the District of Columbia, Puerto Rico, and the Virgin Islands, have legislation in place that requires both private and government entities to notify and inform individuals of any security breaches involving PII.
--- Gordon, Adam. The Official (ISC)2 Guide to the CCSP CBK(Kindle Locations9217-9220). Wiley. Kindle Edition.

Question No: 11
Test performed on an application or software product while it is being executed in memory in an operating system.
A. Static application security testing(SAST)
B. Dynamic application security testing(DAST)
C. Vulnerability assessment
D. Secure code review
Answer: B
Explanation: (DAST) is generally considered a black-box test. where the tool must discover individual execution paths in the application being analyzed.
DAST is used against applications in their running state. DAST is mainly considered effective when testing exposed HTTP and HTML interfaces of web applications.
--- Gordon. Adam. The Official (ISC)2 Guide to the CCSP CBK (Kindle Locations5793-5794). Wiley. Ki

Question No: 12
What is it called when you lose control of the amount of content on your image store?
A. Data Loss
B. Sprawl
C. Media Contention
D. Media Sanitization
Answer: B
Explanation: Sprawl occurs when you lose control of the amount of content on your image store.
Unnecessary images may be created and run. Each additional image running is another potential point of compromise for an attacker.

Question No: 13
What is the term for the assurance that a specific author actually created and sent a specific item to a specific recipient, and that the message was successfully received?
A. Self-signed certificate
B. Secure delivery
C. PKI
D. Non-repudiation
Answer: D
Explanation: Non-repudiation is a service that provides proof of the integrity and origin of data. An authentication that can be asserted to be genuine with high assurance.

Question No: 14
Who is the trusted third party in the "trusted third-party model of federation"?
A. Identity provider
B. Relying Parties
C. End user
D. Token consumer
Answer: A
Explanation: In the trusted third-party model of federation, the identity provider is the trusted third party, and the relying parties are each member organization within the federation.
--- Malisow, Ben. CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide (Kindle Locations4559-4561). Wiley. Kindle Edition.

Question No: 15
Which standard offers guidelines for information security controls applicable to the provision and use of cloud services?
A. ISO 27017
B. ISO 27018
C. ISO 15048
D. ISO 27034
Answer: A
Explanation: ISO 270017 provides guidance on the information security aspects of cloud computing,

recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO 27k standards.

Question No: 16
Logical segmentation of a physical networking gear and isolation of one virtual network of compute and storage from other is called:
A. VLANS
B. Multi-tenancy
C. Multi-data segmentation
Answer: B
Explanation: Thats the characteristic of multi-tenancy where it refers to the notion of hosting multiple cloud tenants on a single host while sharing resources. For instance, a typical host machine can support numerous virtual tenants based on the amount of CPU, RAM, and storage.

Question No: 17
Which of the following is NOT a state of Data?
A. Data in motion
B. Data in encryption
C. Data at rest
D. Data in use
Answer: B
Explanation: This question introduces a doubt in the mind of the candidate.
Data in encryption is not a state of the data and three states of data are Data in motion. Data at rest and Data in use.

Question No: 18
An Indian media company, produces5-minute video of event which is of the most interest to people in US and company can see that80 percent of the downloads are coming from US. However, there are few users who are complaining delay or error while downloading the video in US or other parts of the world. Currently It is hosted in one of the datacentres of cloud service provider in India. What advise will you give to the media company so that, the error can be fixed?
A. Make a shorter video or reduce the size of the video
B. Change the service provider or look for US service provider
C. Request for Content Delivery network storage
D. Rent a server in US and host the video again
Answer: C
Explanation: A content delivery network(CDN) is a system of distributed servers(network) that deliver pages and other Web content to a user. based on the geographic locations of the user. the origin of the webpage and the content delivery server.
CDNs also provide protection from large surges in traffic.

Question No: 19
Which one is NOT considered as one of the building blocks of the cloud computing?
A. MM

B. CPU
C. Clock
D. Networking
Answer: C
Explanation: The question is asking for an exception by using "NOT".
The building blocks of cloud computing are composed of random access memory (RAM). the central processing unit (CPU), storage, and networking.

Question No: 20
Which of the following is the correct group of the Five trust principles as set by the AICPA (the American Institute of CPAs)?
A. Security, Availability, Integrity, Processing confidentiality, Privacy
B. Security, Availability, Processing Integrity, confidentiality, Privacy
C. Security, Availability, Integrity, confidentiality, Privacy
D. Secured processing, Availability, Integrity, confidentiality, Privacy
Answer: B
Explanation: Be careful in answering this type of questions where all options looks similar
The Five trust principles as set by the AICPA (the American Institute of CPAs) are:
Security: The system is protected against unauthorized access, both physical and logical.
Availability: The system is available for operation and use as committed or agreed.
Processing Integrity: System processing is complete, accurate, timely, and authorized.
Confidentiality: Information designated as confidential is protected as committed or agreed.
Privacy: Personal information is collected, used, retained, disclosed, and disposed of in conformity with the provider's privacy policy.
---- Gordon, Adam. The Official (ISC)2 Guide to the CCSP CBK (Kindle Locations2053-2058). Wiley. Kindle Edition.

Question No: 21
Which of the cloud service model has least maintenance or administration from a cloud customer perspective?
A. IaaS
B. PaaS
C. SaaS
D. XaaS

Answer: C
Explanation: SaaS requires least maintenance from the customer as all the infrastructure up to application is managed by the cloud service provider

Question No: 22
In which of the following cloud service models is the customer required to maintain the operating system?
A. PaaS
B. Public Cloud
C. IaaS
D. SaaS

Answer: C
Explanation: According to "The NIST Definition of Cloud Computing," in IaaS, "the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include OSs and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over OSs, storage, and deployed applications; and possibly limited control of select networking components (e.g, host firewalls)." ---- Gordon, Adam. The Official (ISC)2 Guide to the CCSP CBK (Kindle Locations910-914). Wiley. Kindle Edition.

Question No: 23
IS027001 certification can be taken as proof to achieve Third-party assessment level in CSA star program.
A. True
B. False
Answer: A
Explanation: The CSA STAR Certification is a rigorous third-party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix.

Question No: 24
Security communication in HI'-PS is driven by:
A. SSL & SNMP
B. HTTP & SNMP
C. TLS & SNMP
D. SSL & TLS
Answer: D
Explanation: Transport Layer Security(TLS) and its predecessor, Secure Sockets Layer (SSL), both frequently referred to as “SSL”, are cryptographic protocols that provide communications security over a computer network. Websites are able to use TLS to secure all communications between their servers and web browsers

Question No: 25
What is true about REST and SOAP APIs?
A. SOAP is used where bandwidth is limited and REST is used for asynchronous processing
B. REST is used for stateless operations whereas SOAP is used for Stateful Operations
C. REST is heavily reliant on XML
D. REST is highly intolerant about errors
Answer: B
Explanation: Some examples of situations where REST works well are
1. When bandwidth is limited
2. When stateless operations are used
3.When caching is needed
Some examples of where SOAP works or fits in better are
1. Asynchronous processing

2. Format contracts
3. Stateful operations
---- Malisow, Ben. CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide (Kindle Locations4658-4660).Wiley. Kindle Edition.

Question No: 26
Which of the following is NOT atypical approach of Key Storage in cloud?
A. Internally managed
B. Externally managed
C. Cloud Service Provider Managed
D. Managed by the Third part
Answer: C
Explanation: Remember. two key considerations when doing key management
1) Do not save it alongside data
2) Do not let cloud service provider manage the keys

Question No: 27
The relationship between the shareholders (and other stakeholders) of the organisation versus the Senior Management of the organisation is governed by:
A. IT Governance
B. Corporate Governance
C. Corporate Vision
D. Corporate Mission
Answer: B
Explanation: Corporate governance is the system of rules, practices and processes by which a company is directed and controlled. Corporate governance, essentially involves balancing the interests of a company's many stakeholders, such as shareholders, management, customers, suppliers, financiers, government and the community.

Question No: 28
According to ISO 27018, data processor has explicit control over how CSPs are to use PII.
A. True
B. False
Answer: B
Explanation
In ISO27018, it is the customer who has explicit right over how CSPs will use their information.

Question No: 29
Relative values are characterstics of which type of risk assessment?
A. Traditional
B. Quantitative
C. Hybrid
D. Qualitative
Answer: D

Explanation: There are two primary methods of risk analysis you can use on your project…
1. Qualitative Risk Analysis
2. Quantitative Risk Analysis
The main difference between qualitative and quantitative risk analysis is that the former uses a relative or descriptive scale to measure the probability of occurrence whereas quantitative analysis uses a numerical scale. For example. a qualitative analysis would use a scale of "Low. Medium. High" to indicate the likelihood of a risk event occurring.

Question No: 30
Type2 hypervisor is more secure than Type1 hypervisor. Is it true?
A. It is true becauseType2 hypervisor runs as a bare metal
B. It is false asType1 hypervisor is more secure because of reduced attack surface
C. It is true because Type2 hypervisor has reduced attack surface as compared to Type1 Hypervisor
D. Both are same in terms of security
Answer: B
Explanation: Type1 hypervisors significantly reduce the attack surface overType2 hypervisors.
Type1 hypervisor vendors also control relevant software that comprise and form the hypervisor package. Including the virtualization functions and 0S functions. such as devices drivers and input/ output (I/O) stacks. Because the vendors have control over the relevant packages they can reduce the likelihood of malicious software being introduced into the hypervisor foundation and introducing or exposing the hypervisor layer.
--- Gordon. Adam. The Official (ISC)2 Guide to the CCSP CBK (Kindle Locations 1517-1521). Wiley. Kindle Edition.

Question No: 31
Tom visits a website which is injected with a malicious script that steals each visitor's session cookies. The session cookie is stolen and his private information compromised lator. He is victim of:
A. SQL Injection
B. Cross site scripting(XSS)
C. Cross site Forgery Request(CSRF)
D. Teardrop.c
Answer: B
Explanation: He is victim of XSS attack.
Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end.

Question No: 32
Metrics which govern the contractual obligations of cloud service are found in?
A. Contract itself
B. Service Level agreements(SLA)
C. Operational Level Agreement(OLA)
D. Service Book
Answer: B
Explanation: The SLA is the list of defined, specific, numerical metrics that will used to determine whether the